HAZARDS ANALYSIS OF HOLSTON AMMONIUM NITRATE/NITRIC ACID STORAGE AND TRANSFER SYSTEM

W. L. Walker

Hercules, Incorporated

Prepared for:

Holston Army Ammunition Plant

July 1974

HERCULES INCORPORATED
ALLEGANY BALLISTICS LABORATORY
CUMBERLAND, MARYLAND

FINAL REPORT

HAZARDS ANALYSIS OF HOLSTON AMMONIUM NITRATE/NITRIC ACID STORAGE AND TRANSFER SYSTEM

REPORT NO. AO8204-520-11-005

JULY, 1974

W. L. WALKER

FOR

HOLSTON ARMY AMMUNITION PLANT
KINGSPORT, TENNESSEE

CONTRACT NO. 083-0446

HERC NO. 74-136

HERCULES INCORPORATED
ALLEGANY BALLISTICS LABORATORY
CUMBERLAND, MARYLAND

FINAL REPORT

HAZARDS ANALYSIS OF HOLSTON AMMONIUM NITRATE/NITRIC ACID STORAGE AND TRANSFER SYSTEM

REPORT NO. A08204-520-11-005

JULY, 1974

W. L. WALKER

FOR

HOLSTON ARMY AMMUNITION PLANT
KINGSPORT, TENNESSEE

CONTRACT NO. 083-0446

HERC NO. 74-136

EXECUTIVE SUMMARY

Hercules Incorporated has conducted a quantitative hazards and risk analysis on the preliminary design of the proposed ammonium nitrate/nitric acid Transfer facility to be constructed at Holston Army Ammunition Plant.

The evaluation of all potential fire and explosion hazards was accomplished through the application of the Hazards Evaluation and Risk Control (HERC) program developed by Hercules. This is a quantitative technique for assessing process risk and specifically conforms to the requirements of U.S. MUCOM Regulation 385-22, "Safety Hazards Analysis." In addition, system failures and/or fault sequences which could cause a loss of facility operation (spills, blockage, corrosive failure, etc.) were evaluated through a logic modeling technique.

In this report, specific recommendations are offered which, when implemented, would reduce overall system risk in a cost effective manner. These recommendations, generally consisting of minor modifications in equipment design and operating procedures, will serve as a useful guide during the subsequent completion of the facility design.

Relatively small overall fire and explosion probabilities were determined to exist for the Transfer system, as currently designed. This is attributed to: (1) the relative insensitivity of process materials to standard forms of initiation, and (2) the complete lack of an explosive potential existing in the facility during normal operations. Under certain abnormal conditions, identified in the analysis, an explosive potential could be present and in such cases, specific recommendations are offered to reduce the probability of an explosion occurring. The normal and abnormal operation of the proposed electrically heated transfer line was found to contribute only marginally to the overall facility risk.

WARRANTY AND DISCLAIMER

Within the scope of work, Hercules warrants that it has exercised its best efforts in performing the hazards analysis hereunder, but specifically disclaims any warranty, expressed or implied, that any particular standard or criterion of hazard or accident elimination has been achieved by Holston Defense Corporation, if Holston Defense Corporation adopts the findings or recommendations of Hercules.

TABLE OF CONTENTS

	Page
INTRODUCTION	1
SUMMARY	2
A. Objectives	2
B. Results and Conclusions	2
C. Recommendations	5
I. PRELIMINARY HAZARDS ANALYSIS	I-1
A. Process Survey	1
B. Logic Model	1
C. Qualitative Analysis	2
II. MATERIAL RESPONSE	II-1
A. Ammonium Nitrate/Nitric Acid Sensitivity	1
B. Sustained Burning Results	4
C. Transition to Explosion	5
D. Explosive Propagation	6
E. Initiation Probabilities	7
III. ENGINEERING ANALYSIS AND HAZARDS EVALUATION	III-1
A. Introduction	1
B. Summary and Conclusion	1
C. Analysis of Subsystems	1
1. Process Pumps	2
2. Plug and Ball Valves	4
3. Globe and Pressure Relief Valves	4
4. Heated Transfer Line	4
5. Cleanup Operations	5
IV. RISK ANALYSIS	
A. Introduction	IV-1
B. Summary and Conclusions	1
1. Fire/Explosion Hazards	1
2. Reliability	3
C. Fire/Explosion Evaluation	5
1. Probabilistic Approach	5
2. Fire/Explosion Results	9
D. Reliability Evaluation	18
1. Probabilistic Approach	18
2. Reliability Results	19
V. TRADE-OFF STUDY	V-1
VI. BIBLIOGRAPHY	VI-1

TABLE OF CONTENTS (CONTINUED)

	Page
APPENDIX A - LOGIC MODEL	A-1
APPENDIX B - EXPERIMENTAL DISCUSSION	B-1
APPENDIX C - RELIABILITY CALCULATIONS	C-1
APPENDIX D - CALCULATION OF ADIABATIC FLAME TEMPERATURE FOR AN	D-1

LIST OF TABLES

Table No.	Title	Page
I-A	Logic Symbology and Definitions	I-3
I-B	Potential Initiation Modes of a Process Pump	I-4
II-A	Ammonium Nitrate and Ammonium Nitrate/Nitric Acid Sensitivity Summary	II-2
II-B	Transition Test Results	II-6
II-C	Explosion Propagation (Critical Diameter) Test Results	II-7
IV-A	Process Risk Summary - Fire/Explosion	IV-3
IV-B	Process Risk Summary - Reliability Evaluation	IV-4
IV-C	Fire/Explosion Probability Summary for Tank Farms C-3 and C-7	IV-9
IV-D	Jamesbury Ball Valve	IV-11
IV-E	Durco Plug Valve	IV-12
IV-F	Split Body Globe Valve	IV-13
IV-G	Pressure Relief Valve	IV-14
IV-H	Process Pumps	IV-16
IV-I	Failure of Both Tank Farms to Pass Product	IV-19
IV-J	Failure of a Tank at C-3 or C-7	IV-21
IV-K	Heating System Failure of a Tank at C-3 or C-7	IV-22
IV-L	Steam Tracing Failure of Tank Components at C-3 or C-7	IV-22
IV-M	Shutdown of 3" Transfer Line	IV-23
IV-N	Failure of New Pumphouse to Transfer Product	IV-26
IV-O	Failure of New Storage Tank and Heat Exchanger	IV-29

LIST OF FIGURES

Table No.	Title	Page
I-a	Excerpt from Logic Model	I-6
II-a	Transition Test Setup	II-5

INTRODUCTION

This is the sixth and final report for this program under Contract 083-0446 to Holston Defense Corporation (HDC) for a Hazards Analysis of the Ammonium Nitrate/Nitric Acid (AN/NA) Transfer System, including Tank Farms C-3 and C-7. The Transfer System, currently in the design stage, would basically eliminate the need for loading and unloading railroad tank cars and consequently reduce personnel exposure during these operations.

The AN/NA Transfer System consists of: (1) the existing pump house, (2) new 20 foot diameter Storage Tank with Heat Exchanger, (3) new pump house, (4) new impedance heated 3 inch transfer line, and (5) existing C-3 and C-7 Tank Farms (3 tanks each).

The requirements of the Holston Defense Corporation proposal request (W-72-73) specified that a system analysis be performed to identify undesirable events which have been interpreted to be fires, explosion, personnel injury, loss of product through spills, product blockage, corrosion, and system downtime. The occurrence of these events is determined by a numerical (quantitative) engineering analysis of the failures (mechanical, electrical, and human) or normal occurrences (pumping, heating, valve operations and manual cleanup) with respect to the material response of AN/NA material tested at the specific environmental conditions found in the process. Process risks are determined and are provided to HDC management together with information concerning the probability of hazardous or undesirable events occurring and the expected effect on the system from the standpoint of personnel injury, equipment damage/loss, and downtime. This information will facilitate HDC management decisions concerning changes in the design and operating criteria so that the system can be optimized for safety, cost, productivity and quality.

These objectives are generally specified in Army Regulations[1,2] and are specifically stated in USAMUCOM Regulation 385-22, "Safety Hazards Analysis." This regulation outlines the requirements and criteria for establishing and implementing Hazards Analysis techniques for concept, development, and production phases for planned modernization of MM&TE programs for all USAMUCOM installations.

Hercules believes the work objectives have been accomplished through the use of its Hazards Evaluation and Risk Control Program known as HERC. This technique was developed by Hercules in 1958 and has been formally presented[3] and generally accepted throughout the industry as a practical and cost-effective method of evaluating processing hazards. In fact, the

principal concepts of the Hazards Evaluation and Risk Control program have been incorporated in MUCOM 385-22. This approach is quantitative in nature and utilizes a mathematical logic modeling technique in conjunction with engineering measurements of both the "in-process" energy and the response of processed materials to this energy to determine the severity of any hazards (i.e., fires, explosions) or loss of production. These data, coupled with a computer simulation using the logic model as the format, provide the probability that such hazards or losses will occur in the system as designed.

SUMMARY

A. Objectives

The objectives of this work were:

1. Determine the specific system functions or failures which could cause personnel injury or death, damage to facility or equipment, or no product.

2. Evaluate the severity of these specific events; i.e., mechanical and electrical failures, fires, explosions, and toxicity hazards.

3. Determine the probability of occurrence and safety margins of these normal and abnormal hazardous events.

4. Provide design and operating criteria so that the system can be optimized from the standpoint of safety, cost and productivity while maintaining an acceptable level of product quality.

5. Provide management with sufficient information regarding the probability of system failure so that tradeoff decisions can be made concerning risk versus cost.

B. Results and Conclusions

The AN/NA Transfer System has been analyzed utilizing proven HERC techniques as described in the Introduction. This analysis focuses attention on estimating the chance of incurring a catastrophic event and the probable results therefrom to personnel and/or equipment and provides design and operating criteria for the production operation. A catastrophe is defined as a fire or explosion event in which personnel are severely injured or killed or system loss is experienced.

The overall probability of a catastrophic event (explosion) occurring in the facility during 90 days of operation has been determined to be 1.1×10^{-6}. This evaluation is first based upon the inability of the normal process material to support a transition-to-explosion when subjected to a flame stimuli, as demonstrated by transition test data generated during this program. Abnormal conditions, where confined process materials may become intimately mixed with organic material (such as oil), are viewed as being much more able to support an explosive transition, but these conditions have low probabilities of ever occurring. Another situation identified in the analysis by which an explosion potential would be set up in the facility is if confined process material, such as that present in one of the unvented tanks, were to decompose (give off gases) or vaporize rapidly as a result of abnormally high process temperatures. In light of the highly abnormal conditions which must be present before even an explosion potential is available, a relatively low overall explosion probability has been determined to exist. The most likely source of an explosion is from abnormal heat exchanger operation, resulting in process liquid vaporization and subsequent buildup of explosive pressures.

From the analysis it was determined that there is a 1.1×10^{-5} probability that an incident (fire) would occur in the facility during 90 days of operation. This relatively low incident probability results from: (1) the relative insensitivity of the process materials to the standard forms of initiation, and (2) the inability of the process materials to support a fire even when exposed to a highly energetic initiation source. Almost all of this incident probability is associated with normal rubbing at the mechanical seals of the process pumps during shut down during which initiation (decomposition) will normally occur.

During previous material response testing on AN and AN/NA, no impact or friction initiation could be detected even when the highest energy levels available from the testing apparatus were employed. In those cases where in-process impact or frictional energies were found to be higher than the maximum energy level available from the testing apparatus, safety margins and initiation probabilities could not be calculated. In these cases, it has been conservatively assumed that no safety margins would exist and that the initiation probabilities would be 1. Most of these cases involve the normal and abnormal operation of process pumps, where relatively high in-process energies are available.

In those cases where initiation probabilities of 1 were determined to exist, incident (fire) probabilities were concluded to be relatively small. "Initiation" is defined in this analysis to be localized decomposition. In order for an incident to occur, the initiation must be sustained into a fire. Laboratory tests on the process materials indicate that even when highly energetic ignition sources are employed, the materials will not support a fire. These results are supported by burning tests conducted by the Bureau of Mines.

The general design of the impedance heated transfer line was found to have adequate safeguards to prevent excessively high or low product temperatures from being present in the line for any extended period of time. With abnormally high temperatures existing, the major concern would be possible corrosive failure of the piping. Thermal initiation of the process material resulting from high process temperatures could result in a fire or explosion only if the materials were contaminated with organic material, such as oil. The probability of a fire originating at the electrically heated transfer line during normal, abnormal, and cleanup operations has been determined to be an insignificant contributor to the overall 1.1×10^{-5} incident (fire) probability associated with the entire facility.

Several single-point component failures were identified with the operation of the new Storage Tank and Heat Exchanger which could result in abnormal product temperatures existing at the Heat Exchanger. Such failures, if not promptly corrected, would lead to (1) vaporization of process liquid resulting in explosive pressure buildup, or (2) excessive system corrosion or blockage via freezing. The basic problem lies in the fact that the Heat Exchanger control system (temperature transmitter and controller monitoring the Storage Tank temperatures) is essentially isolated from the actual heating operation at the Heat Exchanger. It is recommended that product temperature at the Heat Exchanger be continuously monitored. This would involve installing a temperature transmitter at the Heat Exchanger which would be tied into a temperature indicator on the master control panel.

The Reliability Analysis showed that there is an average probability of .18 of having at least one random system failure occurring during a 90 day operating period which would result in no product being available from both Tank Farms (C-3 and C-7). This probability encompasses over a hundred single point failures, including primary and secondary component failures and human error in equipment adjustment, maintenance, or selection. Many of the electronic sensors, controllers, etc., utilized in the facility are critical to the operation of the facility in the sense that a single failure would lead to a shut down of both Tank Farms.

The three inch Transfer Line (impedance heated) contributes almost 50% to the overall .18 failure probability. This results mainly from the relatively large number of components present in the ten heating units employed at the line. In the analysis it is conservatively assumed that should an abnormally high or low product temperature be indicated to exist in the Transfer Line the line would be shut down.

The Reliability Analysis has been based upon generic component failure rate data, such as that presented in FARADA.[4] The highly corrosive operating environment present in the facility will play an important role in ultimately determining the actual reliability of the system. For this reason, the value of the reliability analysis lies in its ability to identify those areas of the facility which are most critical to the reliable operation of the system. Minimizing the effects which component failures will have on the facility operation can best be effected by maintaining detailed records on component failures and maintenance for future repair.

C. Recommendations

From the analysis of the present design of the AN/NA Transfer System, the following recommendations are made:

(1) The temperature of the material at the Heat Exchanger should be monitored. This can be accomplished by installing a temperature transmitter at the Heat Exchanger which would input into an indicator in Bldg. 330. This setup would significantly reduce the probability of excessive corrosion or product freezing occurring in the Heat Exchanger. In addition, the overall explosion probability for the facility may be reduced by several orders of magnitude.

(2) An emergency pressure relief valve should be installed at the new storage tank. This would reduce the probability of explosive pressures building up as a result of process liquid vaporization (high product temperature which goes uncorrected).

(3) The bayonet steam heater for the Storage Tank which serves as a backup to the Heat Exchanger may be either manually or automatically operated. The important point is that the temperature transmitter and indicator/recorder (which indicate when additional heating is required) should be separate from the Heat Exchanger controls (TT-3 and TIC-3). In this manner, two single point failures which could cause product freezing in the Storage Tank would be eliminated.

(4) Consideration should be given to the possibility of employing a temperature control system for the long steam traced lines. It has been assumed in the system analysis that the normal operation of steam traces would result in acceptable product temperatures. This area should be investigated during the remaining portion of the design program from the standpoint of maximizing reliability.

(5) When operating, cleanup, and maintenance procedures are written, particular emphasis should be placed upon avoiding the accidental introduction of organic materials, such as oil, grease, etc. into the process flow. The small scale introduction of such contaminants could significantly increase the likelihood of an initiation being sustained into a localized fire, whereas massive contamination of process materials would set up a serious explosion potential (Sprengel explosive).

(6) During the cleanup of the impedance-heated transfer line, power to the heating units should be cut off. A protective covering should be placed over exposed electrical wires and other equipment to reduce the likelihood of corrosive damage (shorts, etc.) occurring as a result of sloppy cleanup procedures.

(7) Should a high product temperature be indicated in the impedance-heated transfer line, it is recommended that the power to the particular heating unit be immediately cut off while maintaining constant product flow. Immediately stopping the product flow (via pump shutdown) would increase the likelihood of an initiation occurring in localized hot spots.

(8) It is understood at this time that Holston is considering the use of concrete boxways and steel pipe supports in replacement of currently existing wooden supports. Installing the transfer lines in a concrete boxway (steel supports) would reduce the likelihood of a fire occurring as a result of a leak. Contact between the process materials and organic materials (wooden pipe supports or organic pipe insulation) could result in spontaneous combustion.

(9) Based on explosive propagation (critical diameter) test results, it is recommended that the 4" diameter pipe proposed to connect the new storage tank and new pump house not be employed. If a single 3" pipe is not feasible, from a production standpoint, two parallel pipes (diameter $\leq$ 3") are recommended in place of the single 4" pipe. In this manner, the likelihood of an explosion propagating between the new pump house and storage tank is significantly reduced.

I. PRELIMINARY HAZARDS ANALYSIS

A. Process Survey

The process survey phase of the program consisted of an in-depth review of available design drawings, manufacturers' literature, etc., in order to become intimately familiar with the proposed system, so that system failure could be defined in terms of fire/explosions and reliability. Failure rates of system components such as pumps, valves, sensors, controllers, etc., were determined using sources such as manufacturers' specifications, and established data banks of FARADA[4] and ROME.[5] The data sources were adequate to define the system reliability and thus alleviate the need for any additional component failure rate testing. Individual component failure rates are discussed in more detail under Section IV, Risk Analysis, of this report.

B. Logic Model

The background obtained in the process survey and the assistance of HDC engineering personnel provided the data baseline for the construction of the system logic model.

This technique is a recognized means[6] of augmenting the preliminary hazards analysis by serving as a useful tool in an in-depth evaluation of the system by defining all credible failure modes of the system, whether they be from human, electrical, or mechanical causes or from normal or abnormal system states. The logic model also provides the basic method for analyzing the interrelationships among the various components of the system. The logic model can also function as a useful troubleshooting guide for HDC in the event of system failure, particularly in the control systems, by identifying the systems failure area on the model and determining what the immediate cause(s) or underlying cause(s) are that contribute to the systems failure, thus helping to pinpoint the specific component(s) failure.

The logic model begins with the top undesired event "no product from both Tank Farms" and proceeds through logical steps (gates) backwards through the system to the existing pumphouse at the beginning of the process. By constructing the model in this manner, each component of the system can be evaluated separately in terms of either its own failure or the immediate causes that would contribute to the failure of the component. This technique results in an in-depth systems failure logic that is extremely comprehensive and provides for an accurate account of all credible failures and failure causes of all system components.

The basic symbols used in the construction of the logic model consist of logic gates such as "and," "or," and "inhibit" gates and event representations such as circles, rectangles, diamonds, and houses. These basic symbols are described in Table I-A and the logic diagram itself is shown in its entirety in Appendix A. To present the model in convenient form for inclusion in this report, the author relied heavily on the use of the transfer symbol. This device facilitates the transfer of information from one section of the model to another.

The model depicts two major failure areas that are of primary importance to the overall analysis of the system: (1) loss of production or systems damage resulting from material initiation, fire or explosions, and (2) loss of operation due to human or component failures.

C. Qualitative Analysis

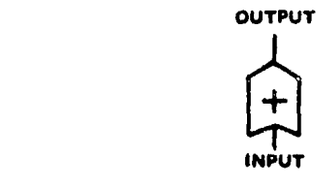
In the qualitative sense, the logic diagram consists mostly of "or" gates and "inhibit" or "sensitivity" gates. Any single failures linked to the top event through "or" gates will cause the top event to occur. For example, failure of TIC-3 (page Q3 of logic model) will result in failure of the system and cause the top undesired event to occur. Over one hundred single factor failure modes were identified from the logic model. The failures identified from the logic model consist of mechanical or electrical components and human factors such as failing to perform functions correctly or doing something at the wrong time. There are also many failures that are common to both the fire/explosion and reliability failure modes such as a pump impeller failure. This aspect of the analysis is discussed in more detail in Section IV of this report.

The failure logic developed for loss of production or system damage resulting from material initiation, fire or explosion, consists of system states that are directly related to component failures, human error, and normal plant operation. Initiation potentials of impact, friction, thermal, and impingement are identified for these system states and have been developed to their fundamental causes. As an example, a listing of the identified potential initiation modes associated with the operation of a process pump is shown in Table I-B. All of the potential initiation modes for each piece of equipment require an engineering analysis to determine ultimate safety margins and initiation probabilities.

TABLE I-A

LOGIC SYMBOLOGY AND DEFINITIONS

LOGIC OPERATIONS

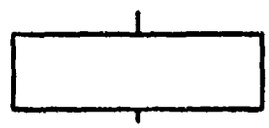


"Or" gates define the situation whereby the output event will exist if one or more of the input events exist.

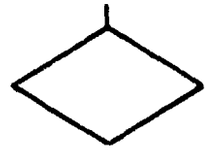
"And" gates describe the logical operation whereby all input events have to occur simultaneously to produce the output event.

"Inhibit" or "Sensitivity" gates describe a causal relationship between one event and another. The input event directly produces the output event if the indicated condition is satisfied.

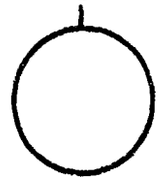
EVENT REPRESENTATIONS



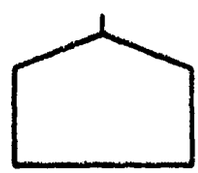
Boxes represent events which are usually expressed as a failure that results from the combination of fault events through the input logic gate.



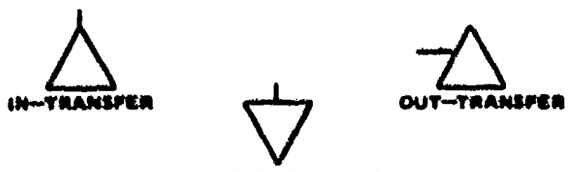
Diamonds represent fault events that are considered basic and define the limit of resolution. The possible causes of the event are not developed either because the event is of insufficient consequence or because the necessary information is not available.



Circles represent basic fault events or primary failures that require no further development. Frequency and mode of failure of items so identified are derived from tests or existing data banks.



Houses represent events that are normally expected to occur such as air being present outside operating vessels.



Triangles are used as transfer symbols to transfer information from one section of the diagram to another.

TABLE I-B

POTENTIAL INITIATION MODES OF A PROCESS PUMP

	Initiation Mode	Description of Event
1.	Friction	Mechanical seal rubbing during startup/shutdown
2.	Thermal	Frictional heating in seal area
3.	Friction	Impeller rubs pump housing
4.	Impact	Impeller impacts pump housing
5.	Friction	Impeller rubs foreign object
6.	Impact	Impeller impacts foreign object
7.	Friction	Impeller rubs layered process solids
8.	Thermal	Shear heating of confined Material
9.	Impingement	Low material level in pump
10.	Friction	Removal of contaminated flange bolts
11.	ESD	Charge buildup on ungrounded operator
12.	Impact	Operator drops nut, bolt, tool into contaminated area

The use of the "inhibit" or "sensitivity" gate provides a means of logically illustrating the in-process conditions that have to be satisfied in order for the failure logic to pass through the inhibit gate. For example, on page L1 of the logic model for the development of the fire/explosion logic for a process pump, the impact energy available due to the pump impeller hitting the pump housing must be compared to the sensitivity of the material to determine the probability of an initiation occurring.

The excerpt from the logic diagram in Figure I-a illustrates the use of the "inhibit" gate. This gate facilitates the computation of the probability of the occurrence of A which is the product of B and C probabilities. The probability of B naturally depends upon the failure logic below it and is eventually keyed in to the probability of the component failures that contribute to B occurring, while the probability of C depends upon the results of the material response test and the in-process impact energy. More explanation of the "inhibit" gate and how the various inputs are developed is given in this report.

The analysis and construction of the logic model for the reliability analysis are analogous to that of the fire/explosion already discussed except there are no sensitivity gates for this analysis. This analysis yielded over 100 modes whose existence would lead to a no-product condition. These failure modes were distributed between mechanical, electrical, and human errors. How each of these components is evaluated and their impact on the system reliability will be discussed in Section IV.

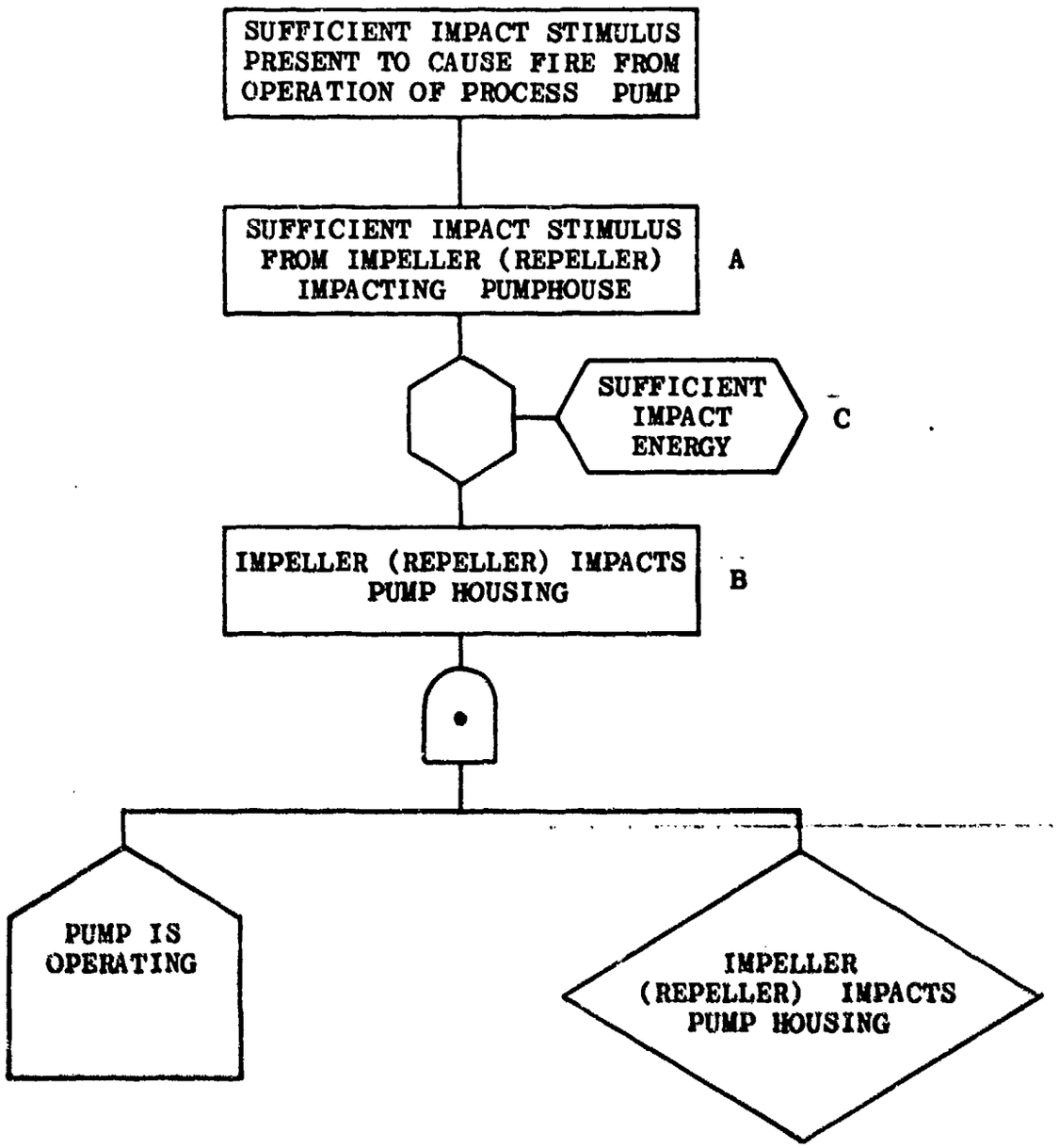


Figure I-a. Excerpt from Logic Model

II. MATERIAL RESPONSE

This section of the report presents the fire and explosion characteristics of the ammonium nitrate/nitric acid (AN/NA) material which will be present in the transfer facility. The sensitivity data, expressed in engineering terms, summarized in this section will be employed in the Engineering Analysis and Hazards Evaluation (Section III) to determine the safety margin associated with each potentially hazardous operation and in the Risk Analysis (Section IV) to determine overall hazard probabilities. Also included in this section is a discussion of the explosive characteristics of AN/NA in terms of its ability to transit to an explosion when exposed to a flame stimuli, as well as its ability to propagage an explosive reaction.

A. Ammonium Nitrate/Nitric Acid Sensitivity

Most of the sensitivity data on ammonium nitrate/nitric acid (AN/NA) employed in this analysis was either generated during recently completed programs [7] [8] for Holston or were available from the Hercules data files. A summary of all of the sensitivity data employed in the analysis is presented in Table II-A.

Both the AN powder and AN/NA solution were found to be relatively insensitive to the standard forms of initiation, except in the case of electrostatic discharge. In fact, no impact or friction initiation could be detected even when the highest energy levels available on the testing apparatus were employed. An ammonium nitrate/oil mixture (95/5) was evaluated in the belief that: (1) oxidizer/organic mixture would be a more sensitive mixture than the ammonium nitrate by itself, and (2) such a mixture could be present in the facility during maintenance/cleanup of pumps, etc. However, the sensitivity levels of even this mixture were beyond the capabilities of the test apparatus, except for ESD where the TIL dropped from 5 joules to 0.5 joules due to the presence of the oil. This difference is not viewed as being highly significant. Testing of the solid AN/NA mixture (unheated) was not deemed necessary due to the relative insensitivity exhibited by pure AN and the AN/oil mixture.

The impact sensitivity data on the AN/NA solution is expressed in Table II-A in terms of an energy rate (ft-lb/sec). From Hercules' extensive research in explosive testing, it has been found that energy rate is the engineering term which best describes the stimulus/reaction characteristic for impact initiation of liquids and slurries. For the impact initiation of solids, in this case AN, the best engineering term has been found to be energy per area ($ft\text{-}lb/in^2$).

TABLE II-A

AMMONIUM NITRATE AND AMMONIUM NITRATE/NITRIC ACID SENSITIVITY SUMMARY

Material	Temperature	Threshold Initiation Level[1]			Electrical Discharge (joules)	Impingement (ft/sec)
		Impact[2]		Friction (psi @ ft/sec)		
		ft-lb/sec	ft-lb/in.^{2}			
AN (Powder)	25°C	--	> 92.5	> 58,000 . 8	> 5	--
AN/Oil (95/5)	25°C	--	> 61.5	> 120,000 . 8	0.5	--
AN/Nitric Acid	40°C	> 177,000	--	> 54,000 . 8	0.075	> 750

(1) TIL - highest test level at which no initiation is detected in 10 or 20 consecutive trials

(2) Engineering term for solids (ft-lb/in.^{2}); for liquids (ft-lb/sec)

Because safety margins (and initiation probabilities) are directly based upon material response data, it is necessary for exact sensitivity data to be available if quantitative safety margins are to be calculated. Since the impact and friction sensitivity data on the ammonium nitrate and AN/NA solution are expressed as "greater than" values, it will be impossible in the hazard analysis to define exact safety margins and quantitative probabilities. This subject will be discussed in greater detail in Section II-E below.

From the standpoint of electrostatic (ESD) initiation, the AN/NA solution was found to be slightly more sensitive than the AN/oil mixture and significantly more sensitive than AN powder. The AN/NA solution was tested at 40°C, the approximate process temperature, whereas testing on the AN and the AN/oil mixture was performed at ambient, simulating clean-up conditions.

At the highest level of the impingement testing apparatus, no initiation was detected. This corresponds to a threshold initiation level of > 750 ft/sec.

The thermal stability of the process materials must be fully characterized in order to accurately assess potential cook-off hazards which may exist in the facility (e.g., pump seal, heated transfer line, etc.). The decomposition temperature for pure AN is reported in the literature[9] to be between 230 and 260°C.

In a recently completed program[7], a DSC trace was run on an AN/oil mixture (95/5) to determine what effect, if any, the presence of a small amount of organic material would have on the thermal stability of ammonium nitrate. In this test, decomposition occurred just slightly above 260°C, which indicated that the organic material had no significant effect upon AN stability. The same results were observed when nitric acid was added to the AN/oil. These results are applicable to the Transfer system since, during maintenance/cleanup, organic material such as oil could be introduced into the process accidentally.

From the thermal data it can be concluded that significant decomposition of AN may be expected to occur in the process should temperatures in excess of 250°C exist. Decomposition, defined as the generation of gases, should not result in a fire, since pure AN will not burn. The burning characteristics of AN are discussed in the next section. Although AN or AN/NA will not burn when initiated, it is reported[10] that AN/oil mixtures ("Sprengel explosive") are capable of burning and sustaining a transition to explosion.

The gases formed during the decomposition of the AN may include highly reactive oxidizers, such as N_2O_4. At the relatively high temperatures required for significant AN decomposition to occur, such gases should react violently with any fuels with which they may come in contact. This again points out the importance of keeping oil, grease, and other fuel contaminants out of the process flow.

B. Sustained Burning Results

An infrared analyzer ("LIRA") was employed in the sensitivity testing to detect when an initiation (decomposition) occurs. If the hazards analysis were based on this data alone, a highly conservative analysis would result since it would be incorrectly assumed that all initiations (decomposition) result in an incident (fire). To determine the likelihood of an initiation being sustained into a fire, sustained burning tests were performed on the AN and AN/NA materials as part of the recently completed D-Building analysis.[8]

It was found that neither the AN nor AN/NA materials sustained a fire when ignited by a highly energetic thermite igniter. By comparing the energy required for initiation (threshold initiation level) determined from the sensitivity testing, to the energy released from the igniter during the burning tests, an energy ratio can be calculated. This ratio is used in this analysis as a rough estimate as to the probability of an initiation sustained into a fire. For AN powder and AN/NA mixture, this probability is calculated to be quite low, about 10^{-6}.

A discussion of the test equipment and procedures employed in these tests is included in the Experimental Section (Appendix B).

These test results are supported by theoretical adiabatic flame temperature calculations on AN (Appendix D) and Bureau of Mines burning tests[11] performed on pure AN. As noted earlier, AN contaminated with oil is reported to be capable of sustaining a fire.

C. Transition-to-Explosion

One extremely important aspect of material response testing is to determine how the AN/NA materials behave under flame conditions at various material confinements. The transition tests were conducted to determine the material height and confinement conditions required for the liquid and solid (frozen) AN/NA materials to promote growth from an ignition stimulus to a transiting explosive reaction. A typical test setup is shown in Figure II-a. The results of the transition testing are summarized in Table II-B.

The results indicate that should a fire develop in the transfer system, the process materials would not readily support a transition to explosion.

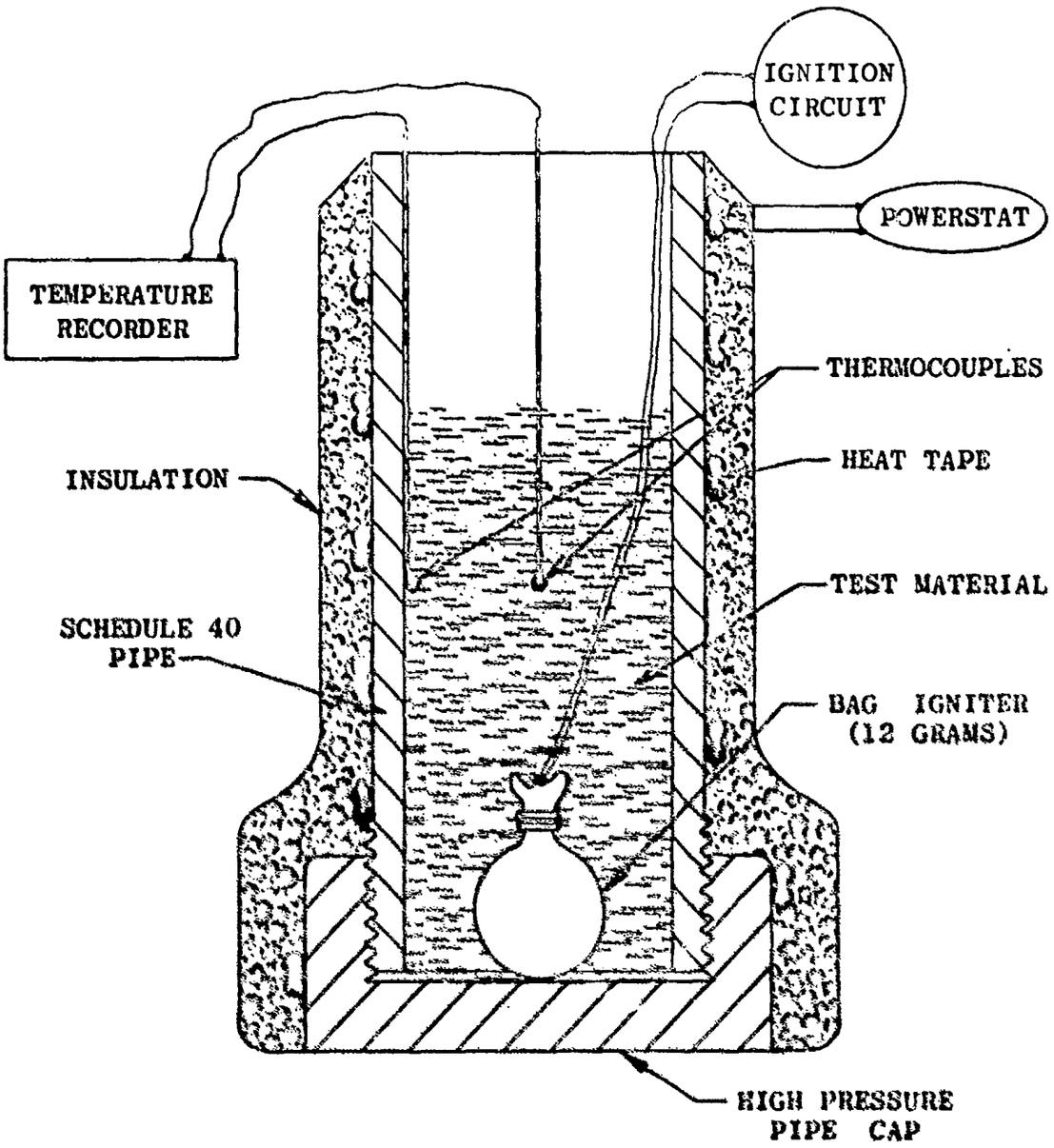


Figure II-a. Transition Test Set-Up

No transition was observed in any of the tests using a 4" diameter Schedule 40 pipe at a material height of 24" in the pipe. Tests were run at both 70°F (solid) and 100°F (liquid) to represent cleanup and operating conditions respectively.

These results are in agreement with previously completed transition test performed at this laboratory on several grades of solid AN. In these tests, no transition was observed in 2" and 4" diameter pipes containing up to 48" of solid AN.

TABLE II-B

TRANSITION TEST RESULTS

	Test Temperature	Confined Diameter	Confined Height	Results
AN/NA liquid	100°F	4"	24"	No reaction
	100°F	4"	24"	No reaction
	100°F	4"	24"	No reaction
AN/NA solid	70°F	4"	24"	No reaction
	70°F	4"	24"	No reaction
	70°F	4"	24"	No reaction

D. Explosive Propagation

Propagation tests were performed on the AN/NA mixture to establish the critical diameter below which the material would not propagate an explosive reaction when exposed to a detonation shock. The results of these tests are used in determining overall system risk, in terms of an explosion in one area of the facility propagating into other areas.

The test results, summarized in Table II-C, indicate that the critical diameter of the confined AN/NA material is between 3" and 4". That is, an explosion occurring in a 3" diameter pipe in the transfer system will not propagate along the pipe whereas a 4" diameter pipe containing AN/NA will support an explosive propagation.

There is only one area in the facility, as currently designed, which will contain piping >3" diameter. This is the process piping connecting the new storage tank with the new pump house. By employing a 3" diameter pipe (or possibly two smaller pipes) in place of the 4" pipe, the probability of an explosion propagating through this pipe would be greatly reduced.

TABLE II-C

EXPLOSIVE PROPAGATION (CRITICAL DIAMETER) TEST RESULTS

Material	Test Temperature (°F)	Critical Diameter (inch)	Results
AN/NA	100	2	No propagation
"	100	3	No propagation
"	100	3	No propagation
"	100	3	No propagation
"	100	4	Propagation, small pipe pieces

E. Initiation Probabilities

Material response data must be treated statistically (i.e., "what is the probability of an initiation at certain input energy levels?") so that material response in probabilistic terms can be applied to the logic model at the "inhibit" gates to facilitate a quantitative analysis of the system logic model. Normally, sensitivity data are plotted on probability paper showing the probability of initiation (percentage of shots) as a function of the amount of stimuli input to the test material; the higher the energy input, the higher the percentage of shots.

This statistical technique has only a limited application to the ammonium nitrate or AN/nitric acid test data since initiations were not detected, even at the highest energy test level, when these materials were exposed to impact and friction stimuli. Only in the case of ESD stimuli were initiations at different test levels detected. Thus, in cases involving impact or friction process conditions, exact initiation probabilities (as well as safety margins) could not be accurately established.

In cases where in-process impact or frictional energies are higher than the maximum energy level available from the test apparatus, it is assumed in the analysis that an initiation probability of 1.0 would exist (with no safety margin existing). In cases where in-process energies are lower than the maximum test level, initiation probabilities are estimated, assuming: (a) the threshold initiation level (TIL) of the material corresponds to the maximum test level, and (b) the relationship between percentage of shots and energy levels (i.e., the "probit slope") is similar to that of other explosives, such as RDX. A line, with this probit slope, is drawn through the data point corresponding to the assumed TIL of the material. The assumptions employed in the estimation of initiation probabilities are viewed as being conservative in nature in the sense that actual initiation probabilities are likely to be less than those presented in this report.

III. ENGINEERING ANALYSIS AND HAZARDS EVALUATION

A. Introduction

The objective of this evaluation is to determine quantitative safety margins associated with each potentially hazardous operation (normal and abnormal) of the facility. A safety margin, defined as

$$\frac{\text{required (material response) energy}}{\text{available (in-process) energy}} - 1,$$

is useful in pointing out those situations, among all of the potentially hazardous events, which are likely to be more hazardous than others if they were to occur. However, in order to assess each potential hazard in terms of risk (expected loss), each event must be evaluated on a probabilistic basis. Such a probabilistic study has been performed and these results are presented in Section IV, Risk Analysis.

B. Summary and Conclusions

The hazards analysis identified several operations (normal and abnormal) where no or only marginal safety margins exist. These situations involve, for the most part, operation of the process pumps where extreme in-process energies are capable of being generated. Under these conditions, the material response data are such that, due to the relative insensitivity of the process materials, it can not clearly be demonstrated that a safety margin exists. The likelihood of an initiation of AN or AN/NA being sustained into a fire, as discussed in Section II, is quite small. Should a fire occur in the system, it is concluded from the transition-to-explosion test data that the incident would not normally develop into an explosion.

A detailed discussion of the Engineering Analysis and Hazards Evaluation performed on the system is presented below. The incident probabilities associated with the potentially hazardous events identified in this analysis were determined as part of the Risk Analysis portion of this program.

C. Analysis of Subsystems

The ammonium nitrate/nitric acid storage and transfer system basically consists of two separate Tank Farms (three tanks each) which are both fed by a 3" diameter, impedance-heated transfer line. Several pumps (in parallel) which feed the transfer line, are supplied with product from a 20-foot diameter storage tank. Material is pumped into the storage tank via the existing pumphouse, containing two parallel pumps. To maintain the product temperature above its freezing point, the transfer line is

impedance heated and the other connecting piping is steam traced. The storge tank is equipped with a heat exchanger (as well as an auxiliary bayonet steam heater), each of the six tanks at the tank farms has its own steam bayonet heater, and the existing and new pumphouses are steam heated. All tanks and lines are insulated with $CaSiO_2$.

1. Process Pumps

At the present design stage of the facility, the selection of a particular pump model to be employed in the new pumphouse has not been made. Analysis of the two candidate pumps, Durco Sealmatic and Wilfley, indicate that similar in-process energies would exist for the operation of the two pumps. Thus, safety margins are concluded to be similar. However, it is impossible to calculate quantitative safety margins for many of the potentially hazardous abnormal situations which may occur during the pumping of the AN/NA material since exact frictional and impact energy levels at which this material (or solid AN) will initiate could not be determined. From previous material testing, as noted earlier, solid AN and the AN/NA material have been found to be relatively insensitive to impact and friction stimuli. The energy levels at which the materials initiate are beyond the energy test level of the laboratory test equipment.

The in-process potentials associated with the centrifugal pumping operations are relatively high and, for the most part, beyond the capability of the laboratory test equipment. A valid analytical technique, applicable to the frictional hazards evaluation of most pumps, is to extrapolate the material response data obtained at several lower velocities to cover a higher range (corresponding to impeller or shaft speeds). This technique is not possible in this particular evaluation since the required pressure levels at the lower velocities are beyond the capability of the test equipment. A similar situation exists, in this particular case, for impact stiuations such as impeller/pump housing or foreign object.

Thus, quantitative safety margins can not be calculated for many of the potential hazards involved in the pumping operation. In such cases, it has been conservatively assumed in this analysis that no safety margins would exist. These situations include:

(1) Friction or impact between impeller (repeller) and housing

(2) Friction or impact between impeller (repeller) and foreign object

(3) Friction between impeller and deposited AN

(4) Rubbing between mechanical seal surfaces

In the above situations, where no safety margins are concluded to exist, the probability of a fire occurring in the pump will depend upon the probability of the initiating event occurring (normal or abnormal) and the probability of the initiation being sustained into a fire. Of the situations listed above, only the one involving rubbing at the mechanical seal will be a normal condition.

For the Durco and Wilfley pumps, rubbing at the mechanical seal interface will only occur during pump startup and shutdown, assuming the pumps are operating as designed. During shutdown, contact at the Durco pump seal begins when the power to the pump is cut off (via solenoid interlock) whereas for the Wilfley pump, seal contact does not occur until the rotating speed of the impeller has slowed (via mechanical governor and spring). In the analysis of both pumps, it has been assumed that velocities at the seal interfaces during contact correspond to the maximum operating velocity of each pump.

Since the mechanical pump seals will not be flushed, solid AN should gradually build up in the seal area. Rubbing in the seal area represents both a frictional and thermal initiation hazard. The frictional in-process potential is 22,000 psi at 14 ft/sec for the Durco pump, this pressure corresponding to the compression yield strength of the carbon insert[12]. For the Wilfley pump, an in-process potential of 3,000 psi (teflon yield strength) at 14 ft/sec would exist. The available material response data on AN indicate that the initiation level is >120,000 psi at 8 ft/sec. From these data, a safety margin can not be calculated. Previous work[13] at this laboratory on mechanical pump seals has indicated that high temperature (> 200°C) can rapidly develop in on-flushed seals, which will be the case here. Ammonium nitrate begins to decompose around 230°C, based on DSC data generated at this laboratory and reported in the literature (Section II). Thus it is concluded that decomposition of AN will normally occur in the mechanical seals of the process pumps present in the facility.

The probability of a fire occurring in the seal area, as a result of friction initiation or thermal decomposition of the AN, is regarded as being quite low based on burning tests performed on AN and AN/NA. However, should an organic contaminant, such as oil, be present in the pump seal area, the chance of a fire occurring as a result of AN initiation is much greater.

Based on the transition-to-explosion test data on solid AN and the AN/NA material, should an initiation occur in a process pump and be sustained into a fire, the fire would not transit to an explosion. As noted in Section II, the process materials were found not to exhibit a transition capability, under the test conditions examined.

2. Plug and Ball Valves

Durco "sleeveline" plug valves will be employed in the pumphouse and storage tank areas. They may also be present at the two Tank Farms, although Jamesbury ball valves are also possible candidates for use in this area.

Comparison of the in-process energies, which may occur during the normal and abnormal operation of the plug and ball valves to the material response data on the process materials indicate positive safety margins to exist. This is attributed to the relative insensitivity of these materials to friction stimuli and to the small in-process potentials which will exist during the operation of these valves.

Comparing the two valves, Durco plug versus Jamesburg ball, it is concluded that similar in-process potentials will be associated with the normal and abnormal operations of each valve. This is due to their close similarity in design, materials of construction, and operation.

3. Globe and Pressure Relief Valves

One globe valve (split body) will be employed at each of the six tanks comprising the C-3 and C-7 Tank Farms as an automatic (air actuated) level control valve. In addition, each tank will have its own pressure relief valve.

Selections of particular valve models have not been made at this particular stage of the facility design. Thus, the analysis was performed on the operation of globe valves and relief valves, in general.

A comparison of in-process potentials to material response data indicate that positive safety margins will exist during the normal and abnormal operation of the globe and relief valves. This can again be attributed to the relative insensitivity of the process materials to friction and impact stimuli and to the small in-process energies associated with the operation of the valves.

As discussed earlier, should a fire occur in one of these valves, a transition-to-explosion would not be likely, based on the transition tests performed on the process materials.

4. Heated Transfer Lines (Electrically and Steam Heated)

The only initiation mode common to both the impedance-heated and steam traced transfer lines is thermal initiation of ammonium nitrate resulting from an abnormally high heat input which goes uncorrected. A

failure in either type of heating line has the potential to cause significant AN decomposition, although a serious fire (or explosion) hazard would only exist if the process materials were contaminated with organic materials, such as oil. The system failures leading to the presence of critically high product temperatures and their associated proabilities are evaluated in Section IV.

Another potential hazard, unique to the operation of the impedance-heated transfer line, is possible ESD initiation caused by an electrical short. Sufficient ESD stimuli from a shorted heating wire would be available for initiation. However, assuming a short does occur, process materials would not normally be exposed to the ESD stimuli. Pipe rupture or poor cleanup operations are two modes by which such exposure could occur. The probability of a fire or explosion occurring under such abnormal conditions is discussed in Section IV.

An additional potential hazard associated with the impedance-heated transfer line is the possibility of an electrolytic reaction occurring inside the pipe as a result of current flowing through the AN/NA solution inself. Calculations, based on reported[19] resistivity values for the process piping and AN/NA, indicate that a relatively small current ($\sim 10^{-2}$ amps) will pass through the AN/NA solution during normal operations. The nature and amount of gas(es) liberated as a result of this electrolytic reaction can only be determined through laboratory testing which simulates actual process conditions. Similar tests would also have to be performed to determine corrosion and product degradation effects. This testing was deemed outside the scope of the present analysis. Because the current flowing through the AN/NA will be relatively small, only minute (if any) amounts of gas will be evolved. If the gases were flammable and were, for example, to gather in a downstream storage tank, an explosion potential would be setup. (An ignition source would be necessary before an explosion would occur). Once the nature of the gas evolution has been determined, flammability tests on the gas mixture could be performed to determine if the gases represent a fire or explosion hazard.

As stated earlier, the quantity of gas formed is expected to be relatively small. For example, assuming hydorgen were evolved as a result of the current flow, approximately 70 in^3 of gas would be formed during a 24-hour period.

5. Cleanup Operations

Only general cleanup procedures, such as the disassembly of valve flanges, were evaluated in this program since specific or detailed procedures were not available for review.

Under normal cleanup conditions, positive safety margins were found to exist. However, under abnormal conditions several situations were found where either no safety margin would exist or where it was impossible to calculate a safety margin, due to the nature of the material response data, as discussed earlier. Included in this latter category are such abnormal situations as: (1) dropping a tool (wrench) onto a contaminated area, or (2) stripping a contaminated flange bolt. Included under the former category is the possibility of charge buildup on an ungrounded person resulting in the ESD initiation of the AN/NA material. Under this abnormal condition, a maximum in-process potential energy of .09 joules could be available, compared to a threshold initiation level of .075 joules for the AN/NA material. The overall probability of an incident occurring under the above abnormal cleanup conditions will be discussed in Section IV.

IV. RISK ANALYSIS

A. INTRODUCTION

This analysis is concerned with quantifying the risks associated with the operation of the ammonium nitrate/nitric acid storage and transfer facility, as currently designed. In this analysis, expected risk has been divided into two general areas: (1) loss of operation due to system failure (reliability), and (2) equipment damage and/or personnel injury (fire/explosion). To determine overall probabilities, a system logic model was constructed and simulated, resulting in the identification of single failures or failure combinations which would result in an undesired event, in terms of reliability or fire/explosion. Once identified, each critical failure mode was evaluated to determine the probability that that particular mode would occur during some operating time period. Each of these probabilities were then summed to determine the overall probability of failure.

The results of the risk analysis are summarized below, followed by a detailed discussion of the analytical techniques employed in the analysis.

B. SUMMARY AND CONCLUSIONS

1. Fire/Explosion Hazards

The analysis indicates that there is a 1.1×10^{-6} probability of a catastrophic event (explosion) occurring in the facility during 90 days of operation. This relatively low probability is attributed to the inability of the process materials to support a transition-to-explosion reaction when exposed to a flame stimuli. Contamination of the AN/NA solution with large amounts of organic material, such as, oil, grease, etc. could set up an explosive potential in the facility due to the in situ formation of a Sprengel explosive. However, a flame (sustained initiation) source would then have to be available under these conditions before an explosion could occur.

The most probable location for an explosion in the facility is at the Heat Exchange area. Rapid AN decomposition (gas evolution) or vaporization of nitric acid in this totally confined area, resulting from abnormally high process temperatures, could cause the buildup of explosive pressures. By monitoring the product temperature at the Heat Exchanger, the overall probability of a catastrophic event occurring in the facility would be reduced by several orders of magnitude.

The probability of an incident (fire) occurring during 90 days of operation has been determined to be 1.1×10^{-5}. This low incident probability is basically due to: (1) the relative insensitivity of the process material to standard forms of initiation, and (2) the demonstrated inability of the process materials to sustain a burning reaction when exposed to a highly energetic ignition source (sustained burning probability of 10^{-6}).

Normal rubbing in the mechanical seals of process pumps during shutdown or startup contributes over 90% to the 1.1×10^{-5} incident probability. For both the DURCO and Wilfley pump models, contact in the seal area will only occur normally during startup or shutdown. During such contact, sufficient frictional and thermal stimuli will be present to cause AN decomposition. However, due to the low sustained burning probability, a relatively low overall incident probability is calculated.

Other situations in the facility were found to be likely sources of AN initiation. However, these conditions were all abnormal (event probability < 1) and were found not to contribute significantly to the overall 1.1×10^{-5} incident probability. Many of these were associated with the abnormal operation of the process pumps (impeller/housing friction, etc.) where relatively large in-process potentials were available.

The impedance heated 3" transfer line was not found to be a significant contributor to the overall incident probability associated with the proposed operation of the facility. The overall probability of a fire occurring in the line as a result of a thermal initiation of the AN has been calculated to be 8.3×10^{-10}. A heating failure(s) would have to occur and go undetected before sufficiently high product temperatures to cause decomposition would be available. The resultant AN initiation would have a very low probability of being sustained into a fire, unless significant amounts of organic material were present in the process stream.

The fire/explosion Risk Analysis is briefly summarized in Table IV-A. The significance of the analysis, in terms of possible design modifications, is discussed in Section V, Tradeoff Study.

Table IV-A

Process Risk Summary - Fire/Explosion

	Overall Probability	
	Incident(1)	Catastrophe(2)
Tank Farms (C-3 and C-7)	8.3×10^{-8}	1.2×10^{-8}
Transfer Line (Electrically Heated)	8.3×10^{-10}	8.3×10^{-16}
New Pump House	6.0×10^{-6}	6.0×10^{-12}
Storage Tank and Heat Exchanger	1.1×10^{-6}	1.1×10^{-6}
Existing Pump House	4.0×10^{-6}	4.0×10^{-12}
Total	1.1×10^{-5}	1.1×10^{-6}

(1) Incident: Fire resulting in slight equipment damage and/or minor personnel injury.

(2) Catastrophe: Explosion resulting in major equipment damage and/or severe personnel injury.

2. Reliability

To briefly summarize the results of the reliability evaluation, it has been determined that there is an average probability of .18 of having one failure (leading to no product from both Tank Farms) occurring during 90 days of operation assuming no maintenance is performed during this time period.

The reliability portion of the logic model was constructed based on the presently conceived design and operation of the facility. Utilizing available component failure rate data, as reported in FARADA,(4) and operator error data (from Hercules' operational files), the probability of a critical system failure occurring was obtained through simulation of the logic model. A critical failure in this analysis has been defined as one which, if it were to occur, would result in no product available from both the C-3 and C-7 Tank Farms. Table IV-B presents a brief summary of the Reliability Analysis.

The three-inch transfer line contributes almost 50% to the overall .18 failure probability. A failure in any one of the ten heating units in the three-inch line could ultimately result in the shutdown of both Tank Farms since excessive or insufficient heating could cause a secondary pipe failure (corrosion) or blockage (product freezing), respectively.

The components in the facility which have the highest reported failure rates are automatic control valves and pumps. Since parallel or auxiliary pumps are present throughout the facility, two or more failures would have to coexist before a critical condition would result. This is also true of the level control valves in the two Tank Farms: at least one valve in each Tank Farm must operate improperly before a shutdown of both farms would result. However, a single (open) failure of the temperature control valve (TCV) at either the heat exchanger of the auxiliary heater (20 ft storage tank) could necessitate a shutdown, if no manual valve were present in the steam lines feeding these TCV's.

Many of the electronic sensors, controllers, etc. utilized in the facility are critical to the operation of the facility in the sense that a single failure could lead to a shutdown of both Tank Farms. Examples of this situation are the electrical components present in the heating units of the three-inch transfer line, as mentioned earlier.

Table IV-B

Process Risk Summary - Reliability Evaluation

Subsystem	Average Probability of Failure During 90 Days Operation
Both Tank Farms	.0198
3" Transfer Line	.0836
New Pump House	.0278
20' Storage Tank	.0268
Existing Pump House	.0255
Overall Average Probability of Failure	.1835

Operator errors will also have a significant influence on the overall reliability of the transfer system. Such errors include: failure to open or close valves as required, improper adjustment of

pumps, failure to notice warning lights/alarms or to take subsequent corrective action, failure to follow prescribed cleanup or maintenance procedures, etc. The deleterious influences which operator errors will have on the system reliability can be minimized through proper training and supervision. With respect to increasing system reliability by reducing mechanical or electrical component failures, several preventive actions are available; e.g., component redundancy, design or procedural modifications, availability of spares, etc. These options will be discussed in a later section of this report (Section V).

Presented in the following section is a detailed discussion of the fire/explosion and reliability evaluation performed in the Risk Analysis.

C. FIRE/EXPLOSION EVALUATION

In this analysis, the probability of a fire or explosion occurring during the normal and abnormal operation of the AN/NA storage and transfer facility was determined. In this manner, the risks associated with the operation of the facility can be evaluated. Should this risk level be found unacceptable, possible corrective action, such as modifying procedures, redesigning equipment, increasing preventive maintenance, etc., can be evaluated in a cost tradeoff study (Section V).

The procedure employed in determining fire and explosion probabilities is presented below, followed by a discussion of the results for each of the subsystems comprising the facility.

1. Probabilistic Approach

a. Incident Probability

An incident in this analysis is defined as the occurrence of an initiation which is sustained into a fire, resulting in loss of product and/or personnel injury. The probability of an incident at a particular point in the facility can be calculated by first identifying the separate events which are necessary to cause the incident (via the logic model), and then determining the probability of each of the events existing at the same time. In equation form, the probability of a single incident (e.g., fire in tank) can be expressed as:

$$P_F = E_p C_p I_p F_p P$$

where: P_F = probability of the incident (fire)

E_p = probability of the initiating event occurring

C_p = probability of combustible material present

I_p = probability of initiation

F_p = probability of the initiation being sustained

F = frequency of occurrence

Each of these terms, as applied to this evaluation, is discussed separately below.

The term "P_F" is technically an expectancy value, as opposed to an actual probability, since frequency (F) is incorporated into the above equation. However, for simplicity, P_F will be termed a probability value throughout this report. The analysis itself is not altered when this nomenclature is employed.

1 Initiating Event (E_p)

All credible events which may lead to an initiation are identified by the construction and simulation of the logic model. The probability of an event occurring (e.g., impeller impacts pump housing) will generally either be time-dependent or time-independent.

Time-dependent events consist of component failures and the probabilities of these events occurring are based on the failure rates of the particular components. A component failure rate, typically expressed in terms of failures per million operating hours, is significantly influenced by the actual environment in which the component must operate. Acceptable failure rate data may be found in such data banks as FARADA[4] or nonelectric failure rate published by ROME Air Development Center.[5] The data from these sources have been tabulated from actual operating records. However, the actual failure rates of components present in a given system will not necessarily be the same, due to differences in operating environments.

Time-independent events can generally be classified as either those which occur normally during an operation (probability equal to one) or those which occur as a result of human error during the operation (probability equal to 10^{-3}). This 10^{-3} value for the probability of human error, derived from Hercules' operational records, means that out of every 1,000 operations which the operator performs, an average of one error can be expected.

The above discussion of event probability (both time-dependent and time-independent) applies equally well to both the fire/explosion analysis and the system reliability prediction.

2 Combustible Material

This is the probability that combustible material will be present in the area when the initiating event occurs. There are a variety of modes by which combustible material could be present in the area of the process under evaluation. These can be generally divided into three cases: (1) normally present (probability equals one), (2) present due to operator error (time-independent, probability equals 10^{-3}), or (3) present due to component(s) failure (time-dependent, probability based on component(s) failure rate). Examples of the three cases above are, respectively: AN/NA material in pump during normal processing, contamination of the area during cleanup, and contamination of valve stem due to seal failure. In some cases, the occurrence of both a component and operator fault is required in order for combustible material to be present. In addition, there are instances where the particular fault causing the initiating event to occur is also responsible for the presence of combustible material (i.e., common cause failure). In these cases, the probability of the combustible material being present is taken to be one, given that the initiating event has occurred.

3 Initiation (I_p)

This is the probability that an initiation will result, given the occurrence of the initiating event (e.g., impeller strikes housing) and the presence of combustible material. An initiation is used in this analysis to mean a decomposition reaction detected by the use of an infrared detector ("LIRA") during material response testing. The probability of an initiation occurring is determined by comparing in-process potentials to material responce data expressed in probabilistic form. This is accomplished by the utilization of the probit technique which has already been described in Section II. In cases where in-process energies are greater than the TIL energy, an initiation probability of 1.0 is conservatively assumed.

4 Initiation Sustainment (F_p)

This is the probability that a sustained burning (fire) will result, given an initiation. This probability is based on supplementary material response testing detailed in Section II. For the AN and AN/NA materials, a sustainment probability of 1×10^{-6} is employed.

5 Frequency of Occurrence (F)

The frequency factor takes into account the number of times the potential initiation event occurs during the 90-day operational time period. In situations involving continuously occurring events (e.g., rotation of agitators or pumps) the frequency factor is defined at 1.0 whereas in cases involving discrete operations or cycles (e.g., closing valve, etc.), then the factor is computed from the number of times the potential initiating event occurs during the 90-day operating period. In this regard, frequency values in this analysis have been based on the facility being started up, operated for 90 days, then shut down to perform the cleanup and maintenance procedures.

b. Catastrophe Probability (P_{cat})

Once the probability of a fire resulting from a particular operation in the process has been calculated (P_F), the probability of a catastrophic event (P_{cat}) occurring from this fire can be determined. In order to do so, the ability of the combustible material to transit to an explosive reaction must be known (R_p). A catastrophe is defined in this analysis to mean an explosive reaction occurring in the facility which would lead to extensive equipment damage and/or severe personnel injury. The probability of a catastrophe occurring at some location in the process is calculated by multiplying the incident probability and the explosion potential together: $P_{cat} = P_F R_p$.

The explosion potential has been concluded in this analysis to be nearly zero ($\leq 10^{-6}$) in cases where normal process materials are exposed to a flame stimuli. This conclusion is based on transition test data which have been summarized in Section II. This is not to say, however, that the generation of explosive pressures in the facility is an absolute impossibility.

For instance, should the AN/NA material be exposed to elevated temperatures, explosive pressures could build up if the vaporization rate exceeded the vent capabilities of the component (e.g., tank) under consideration. Similarly, exposure of solid AN to elevated temperatures (resulting in decomposition) could result in a rupture if the decomposition gases generated were not adequately vented. In this latter example, there is considerable evidence that the rate of AN decomposition increases with pressure as well as with temperature.[10,14] Thus, the rate of decomposition will accelerate as pressure from the inadequately vented gases builds up.

Using the equations and definitions summarized above, the probability of a fire or explosion occurring in the facility during normal and abnormal operations has been calculated. A discussion of the results is presented below.

2. Fire/Explosion Results

a. Tank Farms (C-3 and C-7)

The C-3 and C-7 Tank Farms consist of a total of six steam heated tanks, each having three valves: block, level control, and pressure relief. The analysis indicates that there is an overall probability of 1.2×10^{-8} of a catastrophic event (explosion) occurring at the Tank Farms during a 90-day operating period. Essentially 100% of this value is associated with the buildup of potentially explosive pressures in a tank(s) due to a critically high product temperature (nitric acid vaporization). This would require: (1) failure of both the steam heating system and pressure relief valve of the tank, and (2) the abnormally high temperature (or pressure) to go undetected.

The overall probability of a fire originating at the Tank Farms has been determined to be 8.3×10^{-8}. Most of this probability is associated with the disassembly/assembly of process valves during cleanup or maintenance operations. The normal or abnormal operation of the valves, in general, were found to contribute only marginally to the overall incident probability. This is attributed to the relatively small in-process potentials which will be available. In the analysis, it was assumed that each valve would be cycled once each day and would be disassembled once every 90 days.

The steam tracing operations contribute about 10% to the overall 8.3×10^{-8} fire probability. The probability of a high temperature occurring in one of the steam traced lines is about 6.9×10^{-3} (initiation probability) although a thermal initiation is unlikely to be sustained into a fire, unless organic contaminants are present in the process material.

A summary of the fire/explosion probability analysis performed on the Tank Farms is presented in Table IV-C. Tables IV-D through -G summarize the individual analyses performed on the block valve (DURCO plug of Jamesbury ball), level control valve (split body globe), and pressure valve present at each tank.

Table IV-C

Fire/Explosion Probability Summary
for Tank Farms C-3 and C-7

Equipment	Incident (Fire) Probability	Catastrophe (Explosion) Probability
Block Valves (6)	5.7×10^{-8}	5.7×10^{-14}
Globe Valves (6)	3.5×10^{-9}	3.5×10^{-15}

Table IV-C (Continued)

Fire/Explosion Probability Summary
for Tank Farms C-3 and C-7

Equipment	Incident (Fire) Probability	Catastrophe (Explosion) Probability
Relief Valves (6)	3.0×10^{-9}	3.0×10^{-15}
Steam Tracing	6.9×10^{-9}	6.9×10^{-15}
Tank Heater (6)	1.2×10^{-8}	1.2×10^{-8}
Total	8.3×10^{-8}	1.2×10^{-8}

b. Transfer Line (Impedance Heated)

The 3" transfer line feeding into the C-3 and C-7 Tank Farms will be electrically (impedance) heated using ten individual heating units (thermostat, transformer, etc.). The analysis indicates that there is a relatively low probability of 8.3×10^{-10} of an incident (fire) occurring at the transfer line during a 90-day operating period.

The design of the transfer line is such that in order for a sufficient thermal initiation stimulus to be available, failures in both the heating system and temperature monitoring system would have to coexist. The probability of such a condition occurring has been determined to be quite low (8.3×10^{-4}) due principally to the independent operation of the two systems. Given an initiation, it is unlikely that a burning reaction would be sustained or that the resultant fire would transit into explosion, as discussed earlier.

Another potential initiation mode is electrostatic discharge from a shorted heating wire. The overall probability of an initiation occurring via this mode has been determined to be 1×10^{-6}, which corresponds to an incident probability of 1×10^{-12}.

Should an electrical short or ground failure occur during transfer operations, exposure of the process materials to the ESD stimulu would not occur, unless a pipe failure (rupture) also existed. Simultaneous failures of this nature would most likely be caused by vehicular accidents, falling trees, which result in severe line damage.

TABLE IV-D

JAMESBURY BALL

Potential Hazard	Initiation Mode	Engineering Analysis: In-Process Potential	Engineering Analysis: Material Response	Engineering Analysis: Safety Margin	Frequency/ 2160 hours	Probabilities: Event	Mat'l	Initiation	S.B.	Incident	Transition**	Catastrophe
1. Friction between ball and sleeve	Alloy 20/teflon friction	3,000 psi at 1 ft/sec	>54,000 psi at 8 ft/sec	> 17	90	1.0	1.0	1×10^{-16}	10^{-6}	9×10^{-21}	10^{-6}	9×10^{-27}
2. Friction between ball and housing if seat fails	Alloy 20/steel friction	30,000 psi at 1 ft/sec	>54,000 psi at 8 ft/sec	~ .3	90	10^{-2}	1.0	1×10^{-6}	10^{-6}	9×10^{-13}	10^{-6}	9×10^{-19}
3. Friction between stem and housing should seal leak	Steel/steel friction	42,000 psi at 1 ft/sec	>54,000 psi at 8 ft/sec	~ .3	90	1.0	10^{-2}	1×10^{-3}	10^{-6}	9×10^{-9}	10^{-6}	9×10^{-15}
4. Ball closes on foreign object	Metal/alloy 20 impact	15,000 ft-lb/sec	>180,000 ft-lb/sec	~ 11	90	10^{-3}	1.0	1×10^{-10}	10^{-6}	9×10^{-18}	10^{-6}	9×10^{-24}
	Metal/alloy 20 friction	30,000 psi at 1 ft/sec	>54,000 psi at 8 ft/sec	> .8	90	10^{-3}	1.0	1×10^{-6}	10^{-6}	9×10^{-14}	10^{-6}	9×10^{-20}
5. Foreign object contacts partially opened valve	Metal/alloy 20 impact	45,000 ft-lb/sec	>180,000 ft-lb/sec	> 3.5	90	10^{-3}	1.0	1×10^{-8}	10^{-6}	9×10^{-16}	10^{-6}	9×10^{-22}
	Metal/alloy 20 friction	30,000 psi at 5 ft/sec	>54,000 psi at 8 ft/sec	> .8	90	10^{-3}	1.0	1×10^{-5}	10^{-6}	9×10^{-13}	10^{-6}	9×10^{-20}
6. Cleanup operations												
a. Removal of flange bolts	Steel/steel friction	42,000 psi at 2 ft/sec	>120,000 psi at 8 ft/sec	> .3	4	1.0	10^{-3}	1×10^{-6}	10^{-6}	4×10^{-15}	10^{-6}	4×10^{-21}
Threads are stripped	Steel/steel friction	125,000 psi at 2 ft/sec	>120,000 psi at 8 ft/sec	0*	4	10^{-3}	10^{-3}	~ 1.0	10^{-6}	4×10^{-12}	10^{-6}	4×10^{-18}
b. Charge buildup on ungrounded operator	ESD	6.09 joules	0.971 joules	None	1	10^{-5}	1.0	0.1	10^{-6}	1×10^{-12}	10^{-6}	1×10^{-18}
c. Drop tool upon contaminated area	Steel/steel impact	135,000 ft-lb/sec	>180,000 ft-lb/sec	> .3	10	10^{-3}	1.0	0.5	10^{-6}	5×10^{-10}	10^{-6}	5×10^{-16}

* See Table IV-H

** Probability of significant amounts of organic contaminants in process materials to form Sprengel explosive.

TABLE IV-E

DUKCO PLUG

Potential Hazard	Initiation Mode	Engineering Analysis: In-Process Potential	Engineering Analysis: Material Response	Engineering Analysis: Safety Margin	Frequency/2160 hours	Probabilities: Event	Mat'l	Initiation	S.B.	Incident	Transition**	Catastrophe
1. Friction between plug and sleeve	Alloy 20/teflon friction	3,000 psi at 1 ft/sec	>54,000 psi at ½ ft/sec	~ 17	90	1.0	1.0	1×10^{-16}	10^{-6}	9×10^{-21}	10^{-6}	9×10^{-27}
2. Friction between plug and adjuster if contaminated	Alloy 20/steel friction	30,000 psi at 1 ft/sec	>54,000 psi at ½ ft/sec	> .6	90	1.0	3×10^{-3}	1×10^{-6}	10^{-6}	2.7×10^{-13}	10^{-6}	2.7×10^{-19}
3. Friction between adjuster and grounding spring if contaminated	Steel/steel friction	42,000 psi at 1 ft/sec	>54,000 psi at ½ ft/sec	> .3	90	1.0	3×10^{-3}	1×10^{-3}	10^{-6}	2.7×10^{-10}	10^{-6}	2.7×10^{-16}
4. Friction between plug and housing should sleeve fail	Alloy 20/wall friction	30,000 psi at 1 ft/sec	>54,000 psi at ½ ft/sec	> .6	90	10^{-2}	1.0	1×10^{-6}	10^{-6}	9×10^{-13}	10^{-6}	9×10^{-19}
5. Plug closes on foreign object	Metal/alloy 20 impact	15,000 ft-lb/sec	>182,000 ft-lb/sec	> 11	90	10^{-3}	1.0	1×10^{-10}	10^{-6}	9×10^{-18}	10^{-6}	9×10^{-24}
	Metal/alloy 20 friction	30,000 psi at 1 ft/sec	>54,000 psi at ½ ft/sec	> .6	90	10^{-3}	1.0	1×10^{-6}	10^{-6}	9×10^{-14}	10^{-6}	9×10^{-20}
6. Foreign object contacts partially opened valve	Metal/alloy 20 impact	60,000 ft-lb/sec	>180,000 ft-lb/sec	>3.5	90	10^{-3}	1.0	1×10^{-8}	10^{-6}	9×10^{-16}	10^{-6}	9×10^{-22}
	Metal/alloy 20 friction	30,000 psi at 5 ft/sec	>54,000 psi at 2 ft/sec	> .6	90	10^{-3}	1.0	1×10^{-5}	10^{-6}	9×10^{-13}	10^{-6}	9×10^{-20}
7. Cleanup operations												
A. Removal of flange bolts if contaminated	Steel/steel friction	42,000 psi at 2 ft/sec	>120,000 psi at ½ ft/sec	> .3	4	1.0	10^{-3}	1×10^{-6}	10^{-6}	4×10^{-15}	10^{-6}	4×10^{-21}
Threads are stripped	Steel/steel friction	124,000 psi at 2 ft/sec	>120,000 psi at ½ ft/sec	0*	4	10^{-3}	10^{-3}	~ 1.0	10^{-6}	4×10^{-12}	10^{-6}	4×10^{-18}
B. Charge buildup on ungrounded operator	ESD	0.01 joules	0.075 joules	none	1	10^{-5}	1.0	0.1	10^{-6}	1×10^{-12}	10^{-6}	1×10^{-18}
C. Drop tool upon contaminated area	Steel/steel impact	131,000 ft-lb/sec	>180,000 ft-lb/sec	> .3	10	10^{-3}	1.0	.05	10^{-6}	5×10^{-10}	10^{-6}	5×10^{-16}

* See Table IV-H
** See Table IV-D

TABLE IV-F

SPLIT BODY GLOBE

Potential Hazard	Initiation Mode	Engineering Analysis: In-Process Potential	Engineering Analysis: Material Response	Engineering Analysis: Safety Margin	Frequency/ 2160 hours	Probabilities: Event	Mat'l	Initiation	S.B.	Incident	Transition**	Catastrophe
1. Friction between valve and seat or housing	Alloy 20/teflon friction	1,000 psi at .5 ft/sec	>14,000 psi at 8 ft/sec	> 17	90	1.0	1.0	1×10^{-16}	10^{-6}	9×10^{-21}	10^{-6}	9×10^{-27}
2. Friction between stem and housing	Alloy 20/steel friction	10,000 psi at .5 ft/sec	>14,000 psi at 8 ft/sec	> .6	90	1.0	1.0	1×10^{-6}	10^{-6}	9×10^{-11}	10^{-6}	9×10^{-17}
3. Impact of valve upon seat	Teflon/alloy 20 impact	1,000 ft-lbf/ sec	>150,000 ft-lb/sec	>1.9	90	1.0	1.0	1×10^{-16}	10^{-6}	9×10^{-21}	10^{-6}	9×10^{-27}
4. Valve closes on form an object	Metal/alloy 20 impact	1,000 ft-lbf/ sec	>150,000 ft-lb/sec	> 17	90	10^{-3}	1.0	1×10^{-16}	10^{-6}	9×10^{-24}	10^{-6}	9×10^{-30}
	Metal/alloy 20 friction	10,000 psi at 8 ft/sec	>14,000 psi at 8 ft/sec	> .8	90	10^{-3}	1.0	1×10^{-6}	10^{-6}	9×10^{-14}	10^{-6}	9×10^{-20}
5. Foreign object contacts partially opened valve	Metal/alloy 20 impact	40,000 ft-lb/ sec	>150,000 ft-lb/sec	>5.9	90	10^{-3}	1.0	1×10^{-8}	10^{-6}	9×10^{-16}	10^{-6}	9×10^{-22}
	Metal/alloy 20 friction	10,000 psi at 5 ft/sec	>14,000 psi at 8 ft/sec	> .8	90	10^{-3}	1.0	1×10^{-5}	10^{-6}	9×10^{-13}	10^{-6}	9×10^{-19}
6. Cleanup operations:												
A. Removal of flange bolts if contaminated	Steel/steel friction	42,000 psi at 7 ft/sec	>150,000 psi at 8 ft/sec	> .1	4	1.0	10^{-3}	1×10^{-6}	10^{-6}	4×10^{-15}	10^{-6}	4×10^{-21}
Threads are stripped	Steel/steel friction	126,000 psi at 2 ft/sec	>150,000 psi at 8 ft/sec	0*	4	10^{-3}	10^{-3}	~ 1.0	10^{-6}	4×10^{-12}	10^{-6}	4×10^{-18}
B. Charge buildup on ungrounded operator	ESD	0.04 joules	0.035 joules	none	1	10^{-5}	1.0	0.1	10^{-6}	1×10^{-12}	10^{-6}	1×10^{-18}
C. Drop tool upon contaminated area	Steel/steel impact	135,000 ft-lb/sec	>150,000 ft-lb/sec	> .1	10	10^{-3}	1.0	.05	10^{-6}	5×10^{-10}	10^{-6}	5×10^{-16}

* See Table IV-H
** See Table IV-D

TABLE IV-C

PRESSURE RELIEF

Potential Hazard	Initiation Mode	Engineering Analysis: In-Process Potential	Engineering Analysis: Material Response	Engineering Analysis: Safety Margin	Frequency/ 2160 hours	Probabilities: Event	Mat'l	Initiation	S.B.	Incident	Transition**	Catastrophe
1. Friction between valve and teflon seat	Steel/teflon friction	1,000 psi at .1 ft/sec	>340,000 psi at 8 ft/sec	> 17	90	1.0	1.0	1×10^{-16}	10^{-6}	9×10^{-21}	10^{-6}	9×10^{-27}
2. Impact of valve upon teflon seat	Steel/teflon impact	1,000 ft-lb/sec	>120,000 ft-lb/sec	>179	90	1.0	1.0	1×10^{-16}	10^{-6}	9×10^{-21}	10^{-6}	9×10^{-27}
3. Friction between valve stem and wall should gasket fail	Steel/steel friction	42,000 psi at .1 ft/sec	>54,000 psi at 8 ft/sec	> .3	90	10^{-2}	1.0	1×10^{-16}	10^{-6}	9×10^{-23}	10^{-6}	9×10^{-29}
4. Impact of valve upon wall should teflon seat fail	Steel/steel impact	5,000 ft-lb/sec	>150,000 ft-lb/sec	> 37	90	10^{-2}	1.0	1×10^{-16}	10^{-6}	9×10^{-23}	10^{-6}	9×10^{-29}
5. Cleanup operations												
A. Removal of flange bolts if contaminated	Steel/steel friction	42,000 psi at 2 ft/sec	>110,000 psi at 8 ft/sec	> .3	4	1.0	10^{-3}	1×10^{-6}	10^{-6}	4×10^{-15}	10^{-6}	4×10^{-21}
Threads are stripped	Steel/steel friction	126,000 psi at 2 ft/sec	>120,000 psi at 8 ft/sec	0*	4	10^{-3}	10^{-3}	~ 1.0	10^{-6}	4×10^{-12}	10^{-6}	4×10^{-18}
B. Charge buildup on ungrounded operator	ESD	0.09 joules	0.075 joules	None	1	10^{-5}	1.0	0.1	10^{-6}	1×10^{-12}	10^{-6}	1×10^{-18}
C. Drop tool upon contaminated area	Steel/steel impact	135,000 ft-lb/sec	>180,000 ft-lb/sec	> .3	10	10^{-3}	1.0	.05	10^{-6}	5×10^{-10}	10^{-6}	5×10^{-16}

* See Table IV-H
** See Table IV-D

During cleanup operations, accidental spillage of the corrosive process materials upon heating wire circuitry could result in insulation failure and potential exposure of materials to ESD. However, current would not normally be on during cleanup and, as such, an ESD stimulus would not be available. Failure to clean up spilled materials prior to line startup could result in initiation in shorted areas. Employment of a protective covering over exposed equipment during cleanup operations is recommended as a simple means of reducing the likelihood of an incident occurring as a result of corrosion damage during poor cleanup procedures. These failure modes do not contribute significantly to the overall 8.3×10^{-10} incident probability associated with the transfer line.

c. Pump Houses

An overall probability of an explosion occurring during the 90-day operation of the new pump house (three pumps) has been determined to be 6×10^{-12}, and for the existing pump house (two pumps) it is 4×10^{-12}. Operation of the process pumps were found to be the only significant contributors to these probability values.

As outlined in Section III, initiation (decomposition) will normally occur in the mechanical seals of the process pumps (Wilfley or Durco models). However, initiation of process materials in this area will not readily be sustained into a fire and a transition of this fire into an explosion would require an abnormal condition (organic contaminant of process materials) to exist. These two factors together result in the relatively low overall explosion probability quoted above.

Because initiation will normally occur in the pump seals, abnormal pump operations ("impeller strikes housing," etc.) or valve operations do not contribute significantly to either the fire or explosion hazard probabilities. No significant difference, in terms of incident probabilities, was found between the operation of the Wilfley model and Durco "Sealmatic" model pumps.

The hazards evaluation performed on the operation of the process pumps is summarized in Table IV-H.

The introduction of organic material into the process flow can significantly increase the ability of the process material to sustain an initiation into a fire and support a transition to explosion. Operator error during the maintenance of the process pumps represents the most probable mode by which oil, grease, etc. could accidentelly be introduced into the system. When writing cleanup and maintenance procedures, particular emphasis should be placed upon the avoidance of such errors.

TABLE IV-[illegible]

PROCESS PUMPS

Potential Hazard	Initiation Mode	Engineering Analysis: In-Process Potential	Engineering Analysis: Material Response	Engineering Analysis: Safety Margin	Frequency/ 2100 hours	Probabilities: Event	Mat'l	Initiation	S.B.	Incident	Transition**	Catastrophe
1. Friction between seal surfaces during pump startup/shutdown												
A. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1.0	1.0	~ 1.0	10^{-6}	1×10^{-6}	10^{-6}	1×10^{-12}
	Thermal	[illegible]	[illegible]	None	1	1.0	1.0	1.0	10^{-6}	1×10^{-6}	10^{-6}	1×10^{-12}
B. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1.0	1.0	~ 1.0	10^{-6}	1×10^{-6}	10^{-6}	1×10^{-12}
	Thermal	[illegible]	[illegible]	None	1	1.0	1.0	1.0	10^{-6}	1×10^{-6}	10^{-6}	1×10^{-12}
2. Friction between impeller (or impellers) and housing												
A. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	2×10^{-3}	1.0	~ 1.0	10^{-6}	2×10^{-9}	10^{-6}	2×10^{-15}
B. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	2×10^{-3}	1.0	~ 1.0	10^{-6}	2×10^{-9}	10^{-6}	2×10^{-15}
3. Impact of impeller upon housing												
A. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	2×10^{-3}	1.0	~ 1.0	10^{-6}	2×10^{-9}	10^{-6}	2×10^{-15}
B. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	2×10^{-3}	1.0	~ 1.0	10^{-6}	2×10^{-9}	10^{-6}	2×10^{-15}
4. Friction between impeller and foreign object												
A. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1×10^{-3}	1.0	~ 1.0	10^{-6}	1×10^{-9}	10^{-6}	1×10^{-15}
B. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1×10^{-3}	1.0	~ 1.0	10^{-6}	1×10^{-9}	10^{-6}	1×10^{-15}
5. Impact of impeller upon foreign object												
A. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1×10^{-3}	1.0	~ 1.0	10^{-6}	1×10^{-9}	10^{-6}	1×10^{-15}
B. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1×10^{-3}	1.0	~ 1.0	10^{-6}	1×10^{-9}	10^{-6}	1×10^{-15}
6. Friction between impeller and [illegible]												
A. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1×10^{-3}	1.0	~ 1.0	10^{-6}	1×10^{-9}	10^{-6}	1×10^{-15}
	Thermal	[illegible]	[illegible]	2.4		1×10^{-3}	1.0	10^{-10}	10^{-6}	1×10^{-19}	10^{-6}	1×10^{-25}
B. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1×10^{-3}	1.0	~ 1.0	10^{-6}	1×10^{-9}	10^{-6}	1×10^{-15}
	Thermal	[illegible]	[illegible]	3.0	1	1×10^{-3}	1.0	10^{-10}	10^{-6}	1×10^{-13}	10^{-6}	1×10^{-19}
7. [illegible]	Thermal	[illegible]	[illegible]	1.4	1	1×10^{-3}	1.0	10^{-10}	10^{-6}	1×10^{-19}	10^{-6}	1×10^{-25}
8. [illegible]												
A. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1×10^{-3}	1.0	1×10^{-16}	10^{-6}	1×10^{-25}	10^{-6}	1×10^{-31}
B. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1×10^{-3}	1.0	1×10^{-16}	10^{-6}	1×10^{-25}	10^{-6}	1×10^{-31}
9. Cleaning operations												
A. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	4	1.0	10^{-3}	1×10^{-6}	10^{-6}	4×10^{-15}	10^{-6}	4×10^{-21}
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	6	10^{-3}	10^{-3}	~ 1.0	10^{-6}	4×10^{-12}	10^{-6}	4×10^{-18}
B. [illegible]	[illegible]	[illegible]	[illegible]	None	1	10^{-5}	1.0	0.1	10^{-6}	1×10^{-12}	10^{-6}	1×10^{-18}
C. [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	10	10^{-3}	1.0	.05	10^{-6}	5×10^{-10}	10^{-6}	5×10^{-16}

*U = undetermined safety margin. No initiation of the material [illegible] under the most severe test conditions available. Because in-process potentials are greater than test conditions, a safety margin cannot be calculated. The initiation probability is assumed to be 1.0.
** See Table [illegible]

d. New Storage Tank (with Heat Exchanger)

Process material in the new storage tank will be circulated through a heat exchanger to make up for heat loss during storage. The operation of the storage tank/heat exchanger system contributes essentially 100% to the overall 1.1×10^{-6} explosion probability associated with the 90-day operation of the entire transfer and storage facility.

A catastrophic potential exists in this area should abnormally high process temperatures be generated at the heat exchanger and left uncorrected. Significant vaporization of the process liquid (nitric acid) as well as AN decomposition could occur under such abnormal temperatures. If not corrected, explosive pressures could build up in the enclosed storage tank and heat exchanger.

The failure of either the temperature transmitter (TT-3) at the storage tank or the temperature indicator/controller (TIC-3) which signals the heat exchanger could result in both a critically high process temperature and no corrective action taken. For example, failure of TT-3 could result in a false "low temperature" signal to TIC-3 which, in turn, sends a "heat" signal to the heat exchanger. The operator, observing the temperature on TIC-3, would be unaware of the critically high process temperature. Assuming product was flowing through the impedance-heated transfer line (i.e., Tank Farms not full), the abnormal product temperature could potentially be detected by an operator on the line's temperature indicator. However, shutdown of the heat exchanger would certainly not be an automatic decision and could well be delayed while the transfer line is examined. Similarly, if the Tank Farms were full (no product flowing through the transfer line), the abnormal temperature in the new storage tank/heat exchanger would not be discovered.

The probability of explosive pressures building up in this area can be reduced by several orders of magnitude by monitoring the temperature of the product immediately downstream of the heat exchanger. The temperature indicator (separate from TIC-3) could be installed on the master control panel. In this manner, failure of either TT-3 or TIC-3 could not, by itself, set up a potentially catastrophic condition. As an additional safeguard, a pressure relief valve should be installed on the unvented storage tank.

If sufficient explosive pressure were allowed to build up to rupture the storage tank, this would constitute a Class IV hazard under NUCOM regulation 385-22. Severe equipment damage would result and serious bodily injury from projectiles would occur should personnel be in the immediate tank area.

Monitoring of the heat exchanger temperature would not only reduce the overall explosion probability, but would also reduce the likelihood of excessive corrosion or product blockage (freezing) occurring as a result of abnormal process temperatures which go uncorrected (see Reliability discussion).

D. RELIABILITY EVALUATION

The objective of this evaluation is to determine the overall probability of loss of operation occurring in the AN/NA transfer system. Loss of operation has been defined in this analysis as no product from both Tank Farms C-3 and C-7 for any length of time during a 90-day operating period.

The results of the reliability evaluation indicate that there is an average probability of .18 that at least one failure will occur (mechanical, electrical, or human) during the 90-day operation of the transfer system which will result in no product from both Tank Farms.

The reliability evaluation utilized a system logic model to identify all critical failure modes which could lead to a loss of production. Once identified, the probability of these critical failures occurring were calculated based on typical component failure rate data reported in the literature,[4,5] and human failure rate data derived from Hercules' operational files.

The general results from this analysis, presented in Section IV-B, will not be summarized here. Instead, in the remaining sections, the probabilistic approach employed in the analysis will be discussed followed by detailed discussions on the analysis performed on the various subsystems comprising the transfer system. The reliability section will be followed by a discussion on how to best increase overall system reliability (Section V).

1. Probabilistic Approach

As outlined earlier, the construction and subsequent simultation of the logic model results in the identification of all failure modes (single faults or in combination) which are critical to the operation of the facility in the sense that should any one of them occur, a loss in production operation would result. Included in these faults are equipment malfunction and human error. Once a critical failure mode has been identified, it is necessary to determine the likelihood or probability of that particular failure occurring. By summing all of the separate probabilities together, the overall probability for loss of production can be obtained. This summation technique is valid only in cases where the individual failure mode probabilities are small since no correction is made for cases where two or more critical failure modes may occur simultaneously.

TABLE IV-I

FAILURE OF BOTH TANK FARMS TO PASS PRODUCT

Failure Mode	Typical Failure Rates	Probability of Failure After 2160 Hours
1. Failure of component steam tracing (common cause)		
a. steam pipe failure	1×10^{-8}	2.2×10^{-5}
b. steam header	1×10^{-6}	.0022
c. steam pressure indicator	8×10^{-7}	.0017
d. incorrect installation/selection, etc. of items a, b, and c	NA	.0030
2. Failure of Tank Heaters (common cause)		
a. steam pipe failure	1×10^{-8}	2.2×10^{-5}
b. steam header	1×10^{-6}	.0022
c. steam pressure indicator	8×10^{-7}	.0017
d. incorrect installation/selection/ design of items a, b, and c	NA	.0030
e. incorrect installation/selection/ design of components in tank temperature control system at each tank	NA	.0030
3. Incorrect installation/selection/ maintenance of components listed in Table IV-J	NA	.0200
4. Higher factor failure modes	--	.0008
	Total Probability:	.0396
	Average Propability:	.0198

The probability of a particular failure mode occurring can be determined by evaluating the individual fault or fault combinations comprising the failure. Fault events can generally be classified as either time dependent (component failure) or time independent (human error), as previously discussed in Section IV-B-1. In cases where the failure mode is comprised of a single fault (i.e., single point failure), the probability of the failure mode occurring is the probability of the single fault occurring. In cases where the coexistence of two or more faults is required, the fault probabilities are multiplied together to obtain the failure mode probability.

In cases where a system is found to have numerous single point failure modes, higher order failure modes (i.e., ≥ two faults) can, in most cases, be ignored since their contribution to the overall reliability prediction will be minimal. This is not, however, the general rule when evaluating overall fire/explosion probabilities since it is not only the probability value which is important, but also the consequences (severity of fire, explosion).

Presented below is a discussion of the reliability evaluation performed on the operation of the AN/NA transfer system. For simplification and clarity, the various facility subsystems are discussed separately.

2. Reliability Results

a. Tank Farms (C-3 and C-7)

From the analysis, it has been determined that there is an average probability of .0198 that a failure(s) will occur at the C-3 and C-7 Tank Farms during 90 days of continuous operation such that no product would be available from both Farms. Those component failures and operator faults contributing most significantly to this reliability prediction are discussed below.

The Tank Farms contribute only about 10% to the overall average failure probability of .18 for the entire facility. The relatively high reliability of the Tank Farms can be attributed to the fact that the two Tank Farms operate essentially independently of one another. For both Farms to be shut down, at least one failure would have to exist in each system. The probability of this occurring as a result of primary failures of mechanical (valves, pipes, etc.) or electrical (level transmitters, solenoid valves, etc.) components is extremely remote ($\sim 10^{-4}$) due to their independence. However, secondary failures of such components, brought about by human error, cannot be regarded as independent. Thus, should a level control valve fail at one of three tanks comprising the C-3 Tank Farm due to improper installation

TALLE IV-J

FAILURE OF A TANK AT C-3 OR C-7

	Failure Mode	Typical Failure Rates	Probability of Failure After 2160 Hours
1.	Tank	1×10^{-8}	2.2×10^{-5}
2.	Tank Heating System	(see Table IV-K)	.0215
3.	LCV-7	5.4×10^{-6}	.0117
4.	LCV-7	5.4×10^{-6}	.0117
5.	Relief valve	2.0×10^{-6}	.0043
6.	EV-6	1.8×10^{-6}	.0040
7.	EV-6 Coil	1.0×10^{-6}	.0022
8.	LSHH-7	1.5×10^{-6}	.0032
9.	LIC-6	1.6×10^{-6}	.0035
0.	LT-6	5×10^{-7}	.0011
1.	EV-7	1.8×10^{-6}	.0040
2.	EV-7 Coil	1.0×10^{-6}	.0022
3.	2" Fill line piping	1×10^{-8}	2.2×10^{-5}
4.	2" Fill line flange gasket	1.0×10^{-6}	.0022
5.	2" Fill line flange (loose)	NA	.0010
6.	LAH-6	1.4×10^{-6}	.0030
7.	LAL-6	1.4×10^{-6}	.0030
18.	LSL-6	1.5×10^{-6}	.0032
19.	LAHH-7	1.4×10^{-6}	.0030
20.	P/1-6	8×10^{-7}	.0017
21.	LI-6	5×10^{-7}	.0011
22.	Steam tracing failure (leading to excessive corrosion or product freezing)	(see Table IV-L)	.0069
23.	Incorrect installation/selection/design of above items	NA	.0200
		Probability subtotal:	.1151

TABLE IV-K

HEATING SYSTEM FAILURE OF A TANK AT C-3 or C-7

Failure Mode	Typical Failure Rates	Probability of Failure After 2160 Hours
1. Temperature transmitter	5×10^{-7}	.0011
2. Temperature indicator/controller	1.6×10^{-6}	.0035
3. Temperature control valve	7.9×10^{-6}	.0170
4. Steam pipe failure	1×10^{-8}	2.2×10^{-3}
5. Steam header	1×10^{-6}	.0022
6. Steam pressure indicator	8×10^{-7}	.0017
7. Incorrect installation/selection/ design of above items	NA	.0060
	Total Probability:	.0215

TABLE IV-L

STEAM TRACING FAILURE OF TANK COMPONENTS AT C-3 OR C-7

Failure Mode	Typical Failure Rates	Probability of Failure After 2160 Hours
1. Steam pipe failure (freezing only)	1×10^{-8}	2.2×10^{-5}
2. Steam header	1×10^{-6}	.0022
3. Steam pressure indicator	8×10^{-7}	.0017
4. Incorrect installation/selection/ design of above items	NA	.0030
	Total Probability:	.0069

TABLE IV-M

SHUTDOWN OF 3" TRANSFER LINE

	Typical Failure Rates	Probability of Failure After 2160 Hours
1. Pipe or support (1000) failure	1×10^{-8}	.0220
2. Block valve	2×10^{-6}	.0043
3. Flange gasket	1×10^{-6}	.0022
4. Flange (loose)	NA	.0010
5. Flange (grounded)	NA	.0010
6. Transfer operations halted due to abnormal product temperature indicated in line		
A. TR-5	1×10^{-6}	.0022
B. TT (5A through 5M)	5×10^{-7}	.0132
C. Heating unit thermostat (10)	5×10^{-7}	.0110
D. Heating unit transformer (10)	2×10^{-6}	.0430
E. Heating unit wiring (grounded)	1×10^{-8}	.0002
F. Ground alarm (10)	1×10^{-6}	.0220
7. Incorrect installation/selection/ design of above items	NA	.0450
	Total Probability:	.1671
	Average Probability:	.0836

or maintenance, then it can be reasonably assumed that a similar valve in the C-7 Tank Farm will fail at the same time. Presumably the same person will be involved in the maintenance of similar components present at each Tank Farm. Thus, the secondary failure of the two valves, in this case, can be regarded as a single point failure: human error.

In addition to operator error, other single point or common cause failures were identified from the analysis of the two Tank Farms. These involve the operation of the same steam system supplying the tank heaters of both Tank Farms. A failure in either one of these systems, such as a primary or secondary failure of the steam header, would result in a process upset and the eventual shutdown of both Tank Farms (abnormal product temperature).

At the current design stage of the facility, the selection of a particular valve model for utilization as a level block valve at each tank has not been made. The reliability data available at this time on the two candidate valves (Durco plug and Jamesbury ball) are not sufficient to make a quantitative comparison between the two candidates. However, because of their similarity in design and materials of construction, major differences in reliability would not be expected.

A summary of the reliability analysis on the Tank Farms is presented in Table IV-I.

From typical component failure rate data and human error rates, the probability of any one of the critical failure modes (leading to loss of operation) has been determined for 90 days of operation. The sum of these probabilities equals the overall probability of failure during the time period under evaluation. For the Tank Farms, the probability sum is .0396, as noted in Table IV-I. This means that there is a probability of .0396 of having at least one critical failure occur during a 2160-hour (90 days) operating period. Initially, the overall failure probability will be nearly zero and, as time passes, will steadily increase to .0396 after 2160 hours. Half of the time, the failure probability will be less than .0198 whereas, for the other half of the time, it will be greater than .0198. Thus, the best estimate of the probability becomes the average, or .0198. This technique for calculating the average probability of failure is employed throughout the reliability evaluation.

As a supplementary analysis of the reliability of the Tank Farms, the probability of a failure occurring which would result in one of the six tanks being inoperative was also determined. The results of the analysis, although not applicable to the overall reliability analysis, can serve as a trouble shooting guide by pointing out those

failures which are more likely to occur. The results of the analysis are summarized in Tables IV-J, -K, and -L. Not surprisingly, the .115 average probability of failure results primarily from single point failures of electrical and mechanical components.

b. Three-inch Transfer Line

From the analysis it has been determined that there is an average probability of .0836 that a failure(s) will occur in the 3" transfer line (impedance heated) during 90 days of operation such that no product would be available to both Tank Farms. Shutdown of the transfer line would result in no product being available from the Tank Farms only if the transfer line shutdown lasted for an extended period of time. In the analysis, it is assumed that failures leading to a transfer line shutdown would necessitate an ultimate shutdown of both Tank Farms. Those system failures contributing most significantly to the .0836 failure probability are discussed below.

The impedance heated transfer line contributes almost 50% to the overall average failure probability of .18 for the entire facility. Numerous single point failures could cause the 3" transfer line to be shut down. Most of these are associated with the improper operation of any one of the electrical components which are present in each of the ten individual impedance heating units (thermostat, transformer, ground alarm, etc.) and those which are employed in process monitoring (temperature transmitters and recorder). In the analysis it is assumed that the transfer line would normally be shut down if a critically abnormal product temperature were indicated in the line. An abnormally high ($> 100^{\circ}F$) or low ($< 80^{\circ}F$) product temperature could ultimately cause, if left uncorrected, a secondary pipe failure (corrosion) or blockage (product freezing), respectively.

It would require the occurrence of at least one failure in both the heating and monitoring systems to cause an abnormal product temperature to go uncorrected. Since the two systems will operate and are maintained independently of one another, the probability of two independent system failures occurring under these conditions is quite small ($\sim 10^{-4}$ per 90 days).

A summary of the reliability analysis performed on the transfer line is presented in Table IV-M.

c. New Pump House

From the analysis it has been determined that there is an average probability of .0278 that a failure(s) will occur in the new pump house during 90 days of operation such that no product would be

available to the 3" transfer line. Shutdown of the new pump house would ultimately result in no product being available from the Tank Farms only if the pump house shutdown lasted for an extended period of time. In the analysis, it is conservatively assumed that all failures leading to a pump house shutdown would necessitate an ultimate shutdown of both Tank Farms.

The new pump house contributes only about 15% to the overall average failure probability of .18 for the entire facility. The relatively high reliability can be attributed to the fact that there are three pumps (with associated piping) available for use in the new pump house, whereas the operation of only two of these are absolutely necessary: One pump to recirculate product through the heat exchanger and another pump to supply product to the 3" transfer line. The third pump primarily serves as a backup to the other two, although all three pumps could be used together if required.

Primarily failures of pumps and valves contribute very little to the failure probability of the new pump house operation. At least two out of the three pumping circuits would have to be unavailable before the pump house is shut down. A single failure, which could cause all three pumps to be shut down, is more probable than the simultaneous occurrence of independent failures in two or more of the pumping circuits.

For example, failure of the building heater to supply sufficient heat is a much more likely cause for the pump house being shut down than the primary failure of two pumps. Insufficient heating could be caused by any one of several single component failures (e.g., thermostat, steam control valve, etc.) and would most likely not be noticed before the product freezes in the pipes. The average probability of a critical failure occurring in the building heater has been determined to be about .016 for 90 days of operation, or about 60% of the pump house failure probability. In the analysis, it is assumed that a heater failure will always result in blockage. If the failure were caught before significant freezing in the product line had occurred, a shutdown could be avoided. Discussions with Holston personnel on the existing pump house indicate that failure of the building heater would not necessarily result in blockage via freezing due to: (1) the brief time the product would be in the pump house and (2) secondary heating occurring from the operation of pumps.

Other single point failures identified as potential causes for the shutdown of the pump house include: pipe failure, valve leaks, or human error in adjusting/maintaining pumps, valves, etc. A pipe failure or leaking valve would likely result in an extensive spill, since the operations in the pump house are only infrequently checked by an operator. A secondary failure of all three pumps, for example, could be caused by a single system fault: operator error in adjusting pumps.

Similar considerations apply to the maintenance and adjustment of the manual valves in the pump house.

A summary of the reliability analysis performed on the transfer line is presented in Table IV-N.

At the current design stage of the facility, the selection of a particular pump model for use in the new pump house has not been made. Sufficient failure rate data are not available on the two candidate pumps (Durco "sealmatic" and Wilfley "AF") at this time to make a quantitative comparison between the two. Since similar materials of construction will be employed for each pump, failure via corrosion should not be significantly different between the two pumps. The primary difference in the design of the two pumps is in the mechanism by which the mechanical pump seals are release during pumping. The Wilfley mechanism (mechanical governor) is expected to be slightly more reliable than the Durco mechanism (pressure via solenoid interlock). However, as discussed earlier, primary failures of these pumps will not be as important as, for example, secondary pump failures (incorrect adjustment, etc.) or failure of the building heater. This latter failure would be most critical, with respect to product freezing, during periods when the pumps feeding the transfer line are temporarily shut down as a result of some other system failure.

d. Storage Tank and Heat Exchanger

From the analysis, it has been determined that there is an average probability of .0268 that a failure(s) will occur in the new storage tank or heat exchanger during 90 days of operation such that the new pump house would have to be shut down. Shutdown of the new pump house would result in no product being available from the Tank Farms only if the failure(s) causing the shutdown requires an extended repair time. In the analysis, it is conservatively assumed that all failures leading to a pump house shutdown would necessitate an ultimate shutdown of both Tank Farms. Conditions under which a pump house shutdown would be necessary consist of: (1) high product level indicated, (2) tank or pipe failure (including excessive corrosion), and (3) blockage due to freezing. An indication of an abnormally high or low temperature in the tank would not automatically result in a shutdown.

The new storage tank and heat exchanger contribute less than 20% to the overall average failure probability of .18 for the entire facility. Although a failure of any one component present in the level control system interlocked with existing pump house could cause a shutdown of the storage tank, the .0268 probability value is mostly associated with abnormal heating operations (bayonet heater, heat exchanger, or steam tracing) resulting in product freezing or corrosive failure.

TABLE IV-N

FAILURE OF NEW PUMP HOUSE TO TRANSFER PRODUCT

	Typical Failure Rates	Probability of Failure After 2160 Hours
1. Pipe failure (10)	1×10^{-8}	.0002
2. Manual valves (leaking)	1×10^{-6}	.0132
3. Incorrect installation/selection/ design of pipes or valves	NA	.0070
4. Improper adjustment/maintenance of transfer pumps	NA	.0030
5. Building heater failure (product freezes or excessive corrosion)		
A. Unit heater	1×10^{-8}	2.2×10^{-5}
B. Steam control valve	7.9×10^{-6}	.0170
C. Thermostat	5×10^{-7}	.0110
D. Steam pipe failure	1×10^{-8}	2.2×10^{-5}
E. Incorrect installation/selection/ design of heater components	NA	.0040
6. Higher factor failure modes	--	.0004
	Total Probability:	.0556
	Average Propability:	.0278

A failure in the heat exchanger (insufficient heating) would ultimately result in the process materials freezing if the backup bayonet heater were either not turned on (manually) or failed to deliver sufficient heat when turned on. A failure of either the temperature transmitter (TT-3) or temperature indicator (TIC-3) to operate properly could result in both the heat exchanger delivering insufficient heat and the operator being unaware of the low product temperature. Under these conditions, the bayonet heater would not be turned on by the operator and the product would eventually freeze. Thus, it is recommended that a separate temperature transmitter and indicator be utilized in the operation of the bayonet heater. This could be the same equipment employed in the monitoring of the heat exchanger operation discussed below.

Other single point failures which could cause product freezing are associated with the common steam supply system feeding both the heat exchanger and back-up bayonet heater. Failure of the steam header, pressure indicator, or pipes would fall under this category.

Several two factor failure modes were identified as possible causes of product freezing, although these were found to be relatively insignificant contributors to the overall failure probability. An example of such a failure mode is a primary failure of the temperature control valve at the heat exchanger and failure of the operator to notice the low temperature reading on TIC-3.

With respect to potential overheating problems, it has been assumed in the analysis that should an abnormally high product temperature be indicated in the storage tank, the new pump house would not be shut down. This would depend largely upon the extent of repairs required to correct the indicated high temperature. The single most likely cause of a high product temperature is failure of the temperature control valve (TCV-3) at the heat exchanger, although other single point failures were identified. Should the operator be unaware of the high product temperature, thus allowing the problem to go uncorrected, a secondary failure of the tank or pipes would ultimately occur due to excessive corrosion. This condition is included in the reliability analysis of the storage tank operation since it would necessitate the new pump house to be shut down.

Corrosive failure resulting from an abnormally high product temperature which goes undetected by the operator would require, in most cases, a failure in both the heating system and temperature monitoring system. Failure of the temperature transmitter (TT-3) or indicator/controller (TIC-3) could result in excessive heating from TCV-3 as well as causing the operator to be unaware of the high product temperature.

Should TCV-3 fail open, with everything else operating normally, the temperature of the product in the storage tank would only gradually increase (as measured by TT-3) whereas the temperature in the output line coming from the heat exchanger would be at a critically high level. Under these conditions, excessive corrosion of the line would occur although pipe failure would not be expected unless the high product temperature existed for an extended period of time (> 1 day). Thus, a failure in the temperature monitoring system (TT-3, TIC-3, operator error) would be required before seriously abnormal corrosion would occur.

A summary of the reliability analysis performed on the storage tank and heat exchanger is presented in Table IV-0.

Since there is presently no monitor on the temperature of product coming out of the heat exchanger, excessive corrosion (high product temperature) of the heat exchanger and downstream piping would go uncorrected if the temperature of the bulk material in the storage tank were measured as being normal. Such a condition could be brought about through a variety of conditions: improper design, poor tank or pipe insulation, lower-than-expected outside temperatures, steam tracing failure to supply sufficient heat, etc. Because the product temperature is such a critical factor in the reliable operation of the facility, it is necessary that the operation of the heat exchanger be closely monitored. It is recommended that a temperature transmitter be installed immediately downstream from the heat exchanger which would feed a temperature indicator in Building 330. In this manner, abnormal product temperatures could be rapidly detected. In fact, the temperature differential between the storage tank and heat exchanger could be employed as an indirect indicator of a failure in the steam tracing system, ineffectiveness of the tank or pipe insulation, blockage in the circulation product line, or failure of the recirculation pump in the new pump house. This recommendation has already been made in terms of significantly reducing the overall probability of an explosion occurring in the storage tank/heat exchanger area.

e. Existing Pump House

The reliability analysis on the existing pump house was similar to that performed on the new pump house and from it, an average failure probability of .0255 was calculated to exist for 90 days of operation. Shutdown of the existing pump house would ultimately result in no product being available from the Tank Farms only if the pump house shutdown lasted for an extended period of time. In the analysis, it is conservatively assumed that all failures leading to a pump house shutdown would necessitate an ultimate shutdown of the Tank Farms.

TABLE IV-O

FAILURE AT NEW STORAGE TANK AND HEAT EXCHANGER

	Typical Failure Rates	Probability of Failure After 2160 Hours
.. Tank failure	1×10^{-8}	2.2×10^{-5}
2. LSH-1	2×10^{-6}	.0043
3. LSHH-2	2×10^{-6}	.0043
4. LSHH-2 probe	1×10^{-6}	.0022
5. LT-1	5×10^{-7}	.0011
6. LI-1	5×10^{-7}	.0011
7. Product freezes due to heat exchanger failure and bayonet heater failures (or not turned on)		
A. TT-3	5×10^{-7}	.0011
B. TIC-3	1.6×10^{-6}	.0035
C. Steam pipe failure	1×10^{-8}	2.2×10^{-5}
D. Steam header	1×10^{-6}	.0022
E. Steam pressure indicator	8×10^{-7}	.0017
F. Higher factor failure modes	--	.0001
8. Abnormally high product temperature causing secondary failure of equipment (excessive corrosion)		
A. TT-3	5×10^{-7}	.0011*
B. TIC-3	1.6×10^{-6}	.0035*
C. Steam tracing failure	(see Table IV-I)	.0069
D. Higher factor failure modes	--	.0001
9. Incorrect installation/selection/ design of above items	NA	.0120
	Total Probability:	.0536
	Average Probability:	.0268

* Failure probability already included in item 7 above.

As with the new pump house, primary failure of the pumps and valves were found to contribute very little to the failure probability associated with the existing pump house. This is mainly due to the fact that both pumping circuits would have to be unavailable before the pump house would be shut down. Thus, a single failure, which could cause both pumps to be shut down, is more probable than the simultaneous occurrence of independent failures in both pumps. Due to the similarities in the operation of the existing and new pump houses, the reader is directed toward the discussion of the new pump house operation (Section IV-D-2-c).

V. TRADE-OFF STUDY

Cost trade-off analysis is normally the integrating factor for the fire/explosion and the reliability analysis. This trade-off study attempts to minimize cost, in terms of the losses resulting from catastrophic events and the losses incurred when the facility is shutdown, by increasing safety or reliability. The expenditures associated with these potential changes are traded off against the costs incurred when the system is down as a result of failure.

Based on the proposed design and operation of the AN/NA Transfer system, an overall explosion probability of 1.1×10^{-6} has been determined to exist. Any reduction in this relatively low explosion probability value, through process modifications, increased preventative maintenance, etc., would be more than offset by the increased costs associated with such modifications. Thus, any modifications in process design, maintenance schedules, etc., would not be cost effective in terms of reducing losses associated with a catastrophic event.

The recommendations put forth in the Summary section of this report consist mostly of minor procedural modifications which if followed would significantly reduce the overall probability of a catastrophic event occurring in the facility from a level which is already relatively low. No, or only a marginal, increase in operating costs would be associated with many of these recommendations. The only major modification recommended in the facility design consists of temperature monitoring of the product at the heat exchanger. The equipment involved would add very little to the overall cost of the facility, but would significantly reduce the overall probability of an explosion occurring in the facility from a level which is already relatively low. In addition, such a modification would reduce the likelihood of excessive corrosion or process blockage (product freezing) occurring at the heat exchanger and storage tank as a result of an abnormal process temperature.

In order to effectively reduce costs associated with system unreliability, accurate failure rate data must be available on the components operating in the actual AN/NA transfer system environment. This can best be obtained by keeping careful and complete maintenance records. From these operational records, reliability may be increased via availability of spares and/or increased maintenance.

VI. BIBLIOGRAPHY

1. "Safety for Systems, Associated Subsystems and Equipment," AR-385 (Revision 1).

2. "Safety Manual," AMCR-385-100.

3. R. H. Richardson, et al, "Hazards Analysis Through Quantitative Interpretation of Sensitivity Testing," Presented to the New York Academy of Sciences, Vol. 152, Article 1, October 28, 1968, pp. 269-282.

4. Failure Rate Data Handbook, Naval Fleet Missile System Analysis and Evaluation Group, Corona, California, September 1970.

5. Data Collected for Nonelectronic Reliability Handbook, Volumes II and III, Section I, Report No. RADC-TR-68-14, Rome Air Development, New York, June 1968.

6. C. A. Ericson, "Preliminary Hazards Analysis," Document No. D2-113-072-1, The Boeing Company, 1969, p. 10.

7. L. R. Albaugh, "Hazards Analysis of Holston AOP," HDC P.O. 083-0022, ABL Final Report, March 1974.

8. W. L. Walker, "Hazards Analysis of Holston D Bldg.," HDC P.O. 102-0103-000-A, Final Report, July 1974.

9. G. S. Scott and R. L. Grant, "Ammonium Nitrate: Its properties and Fire and Explosion Hazards," Bureau of Mines Circular, June 1948.

10. Bureau of Mines Report Investigation No. 4994, August 1953.

11. Bureau of Mines, Report Investigation No. 6773, 1966.

12. DuraSeal Manual, 5th Edition, Durametallic Corp., Kalamazoo, Mich.

13. J. DeGiovanni and D. Smith, "Hazards Analysis of a Centrifugal Pump," HDC P.O. 080-0265, ABL Final Report, November 1971.

14. G. Feick and R. Haines, "On the Thermal Decomposition of Ammonium Nitrate Steady-State Reaction, Temperatures and Reaction Rate," Journal of the American Chemical Society, June 14, 1954.

15. "Chemical Rocket/Propellant Hazards," Chemical Propulsion Information Agency Publication 194, Volume II, May 1970, JANAF Hazards Working Group (DOD & NASA).

16. B. Wood and H. Wise, "Kinetics of Thermal Decomposition of Ammonium Nitrate," JPL, California Institute of Technology, January 29, 1954.

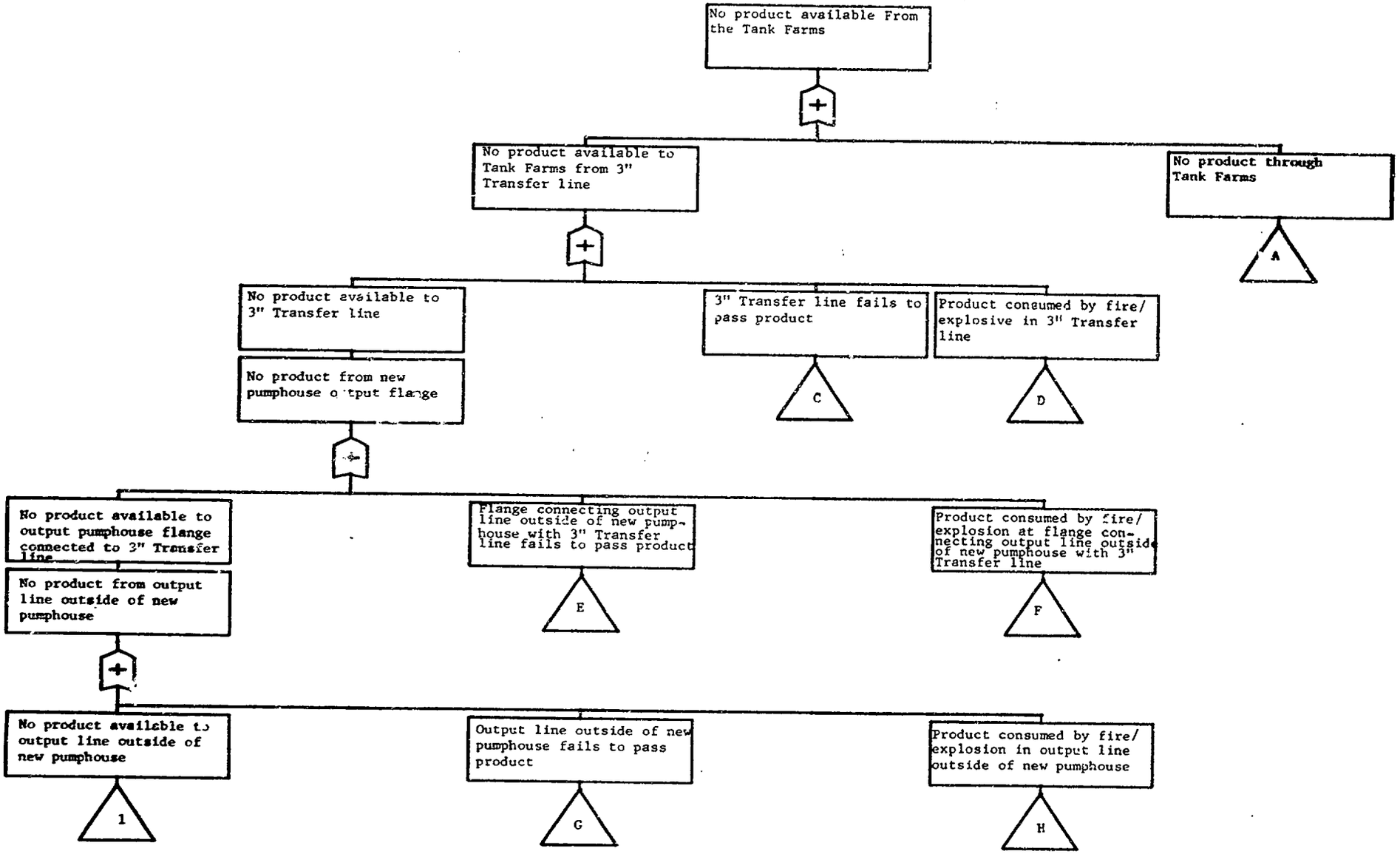
17. R. W. VanDolah and D. L. Burgess, "Explosion Problems in the Chemical Industry," American Chemical Society Publication, 1970.

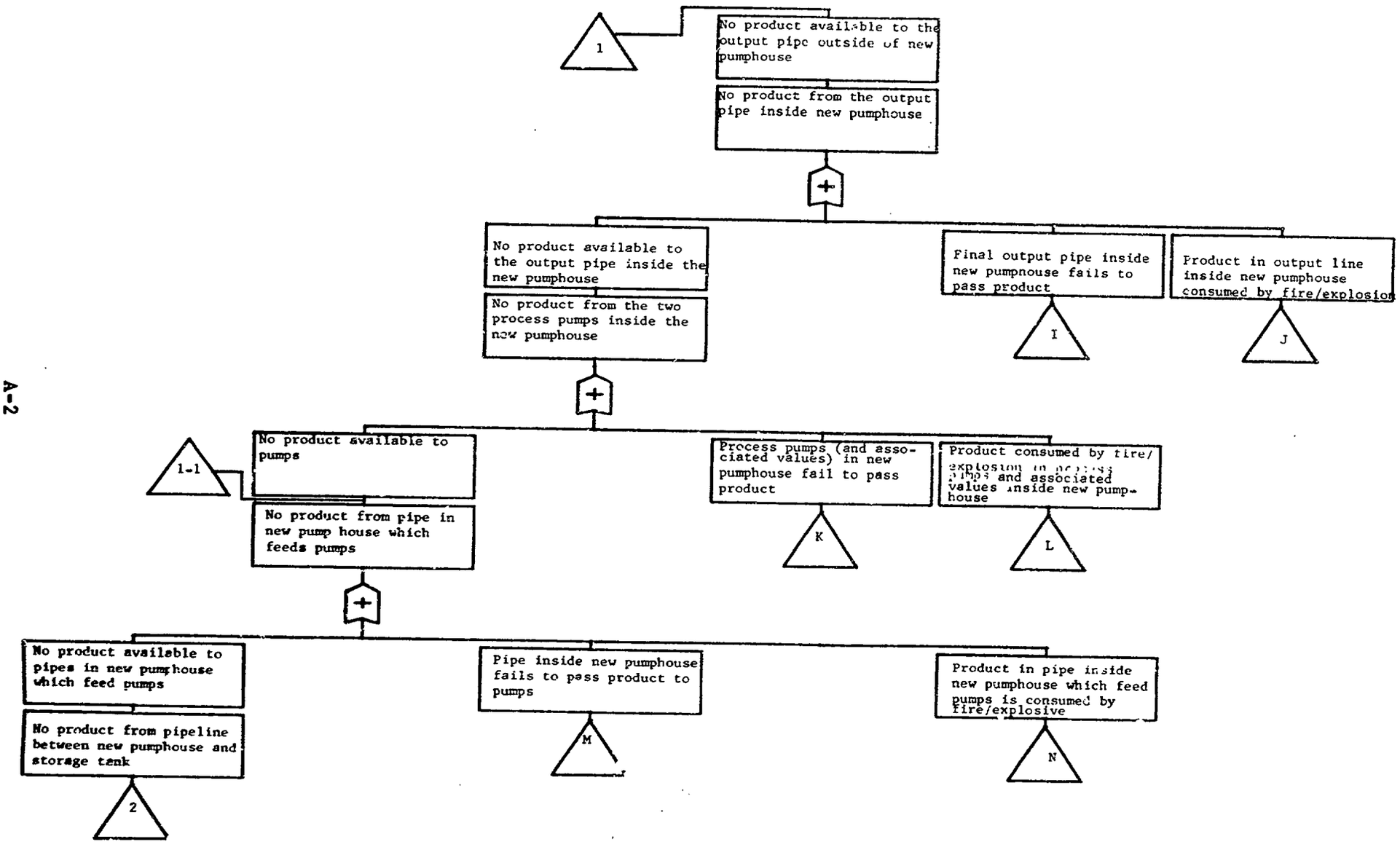
18. N. H. Roberts, "The $\lambda\tau$ Method for Fault Tree Evaluation," February 1969.

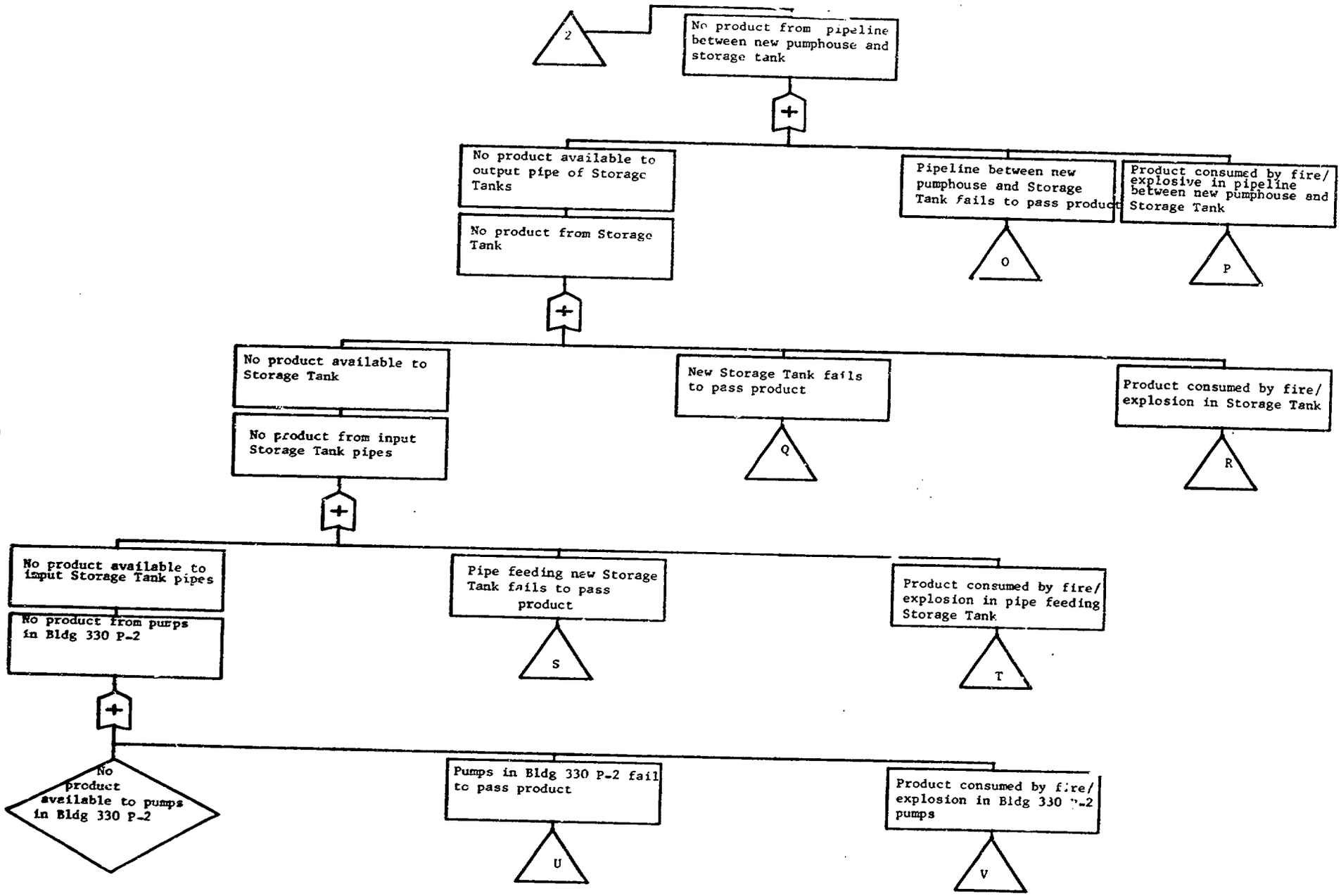
19. "Design Analysis and Calculations," Patchen, Mingledorff and Associates, Contract DACA01-73-C-107 for Holston.

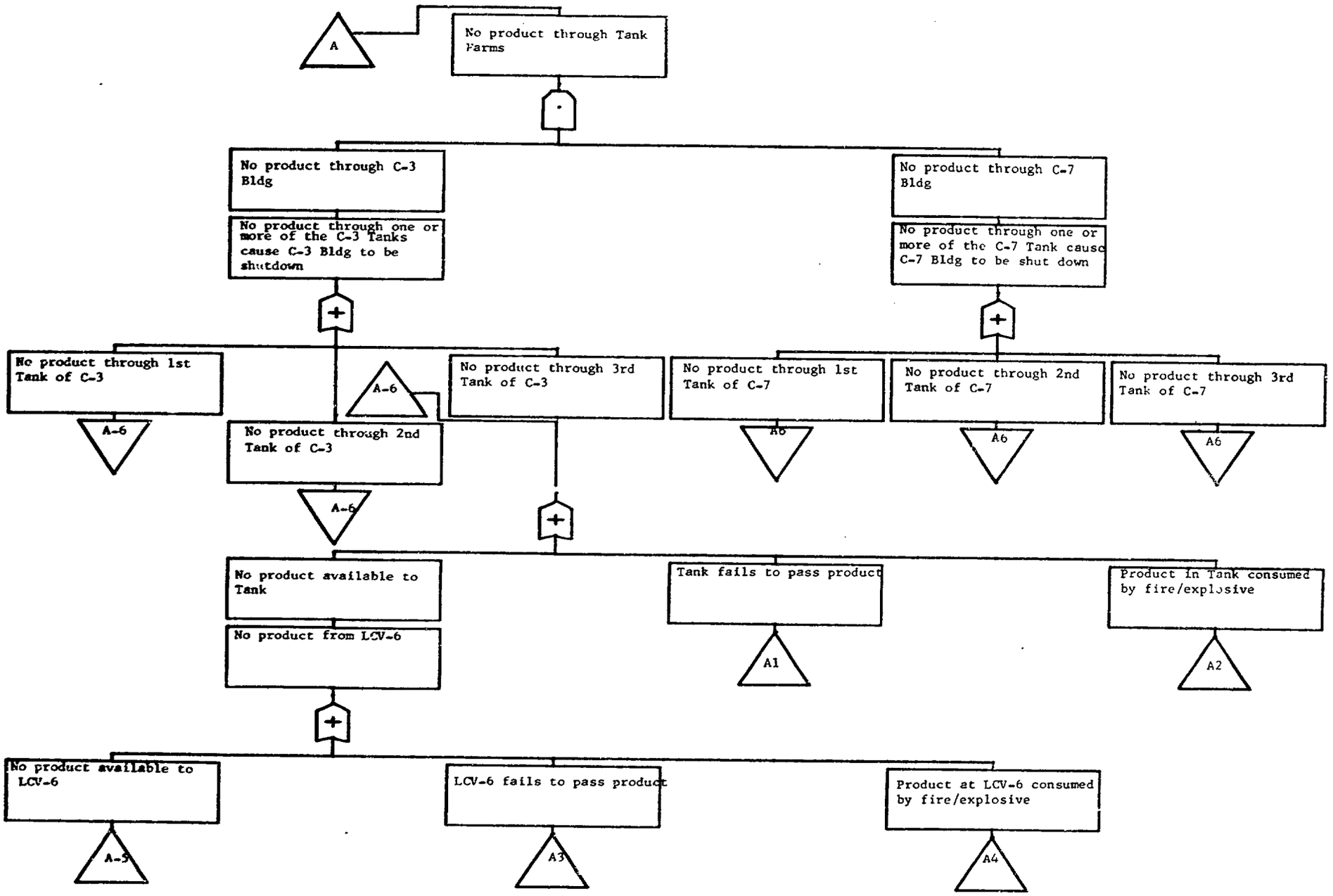
APPENDIX A

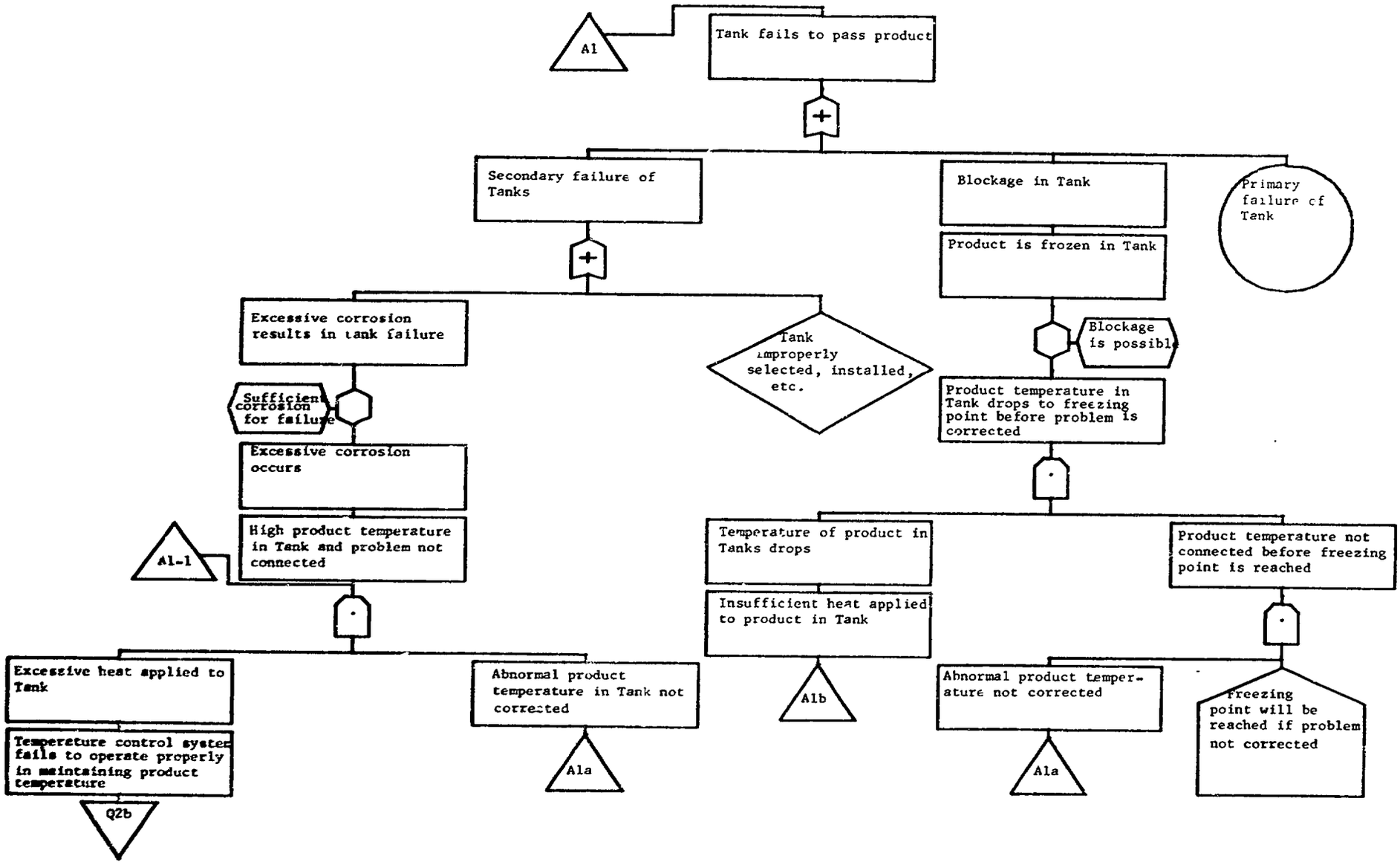
LOGIC MODEL

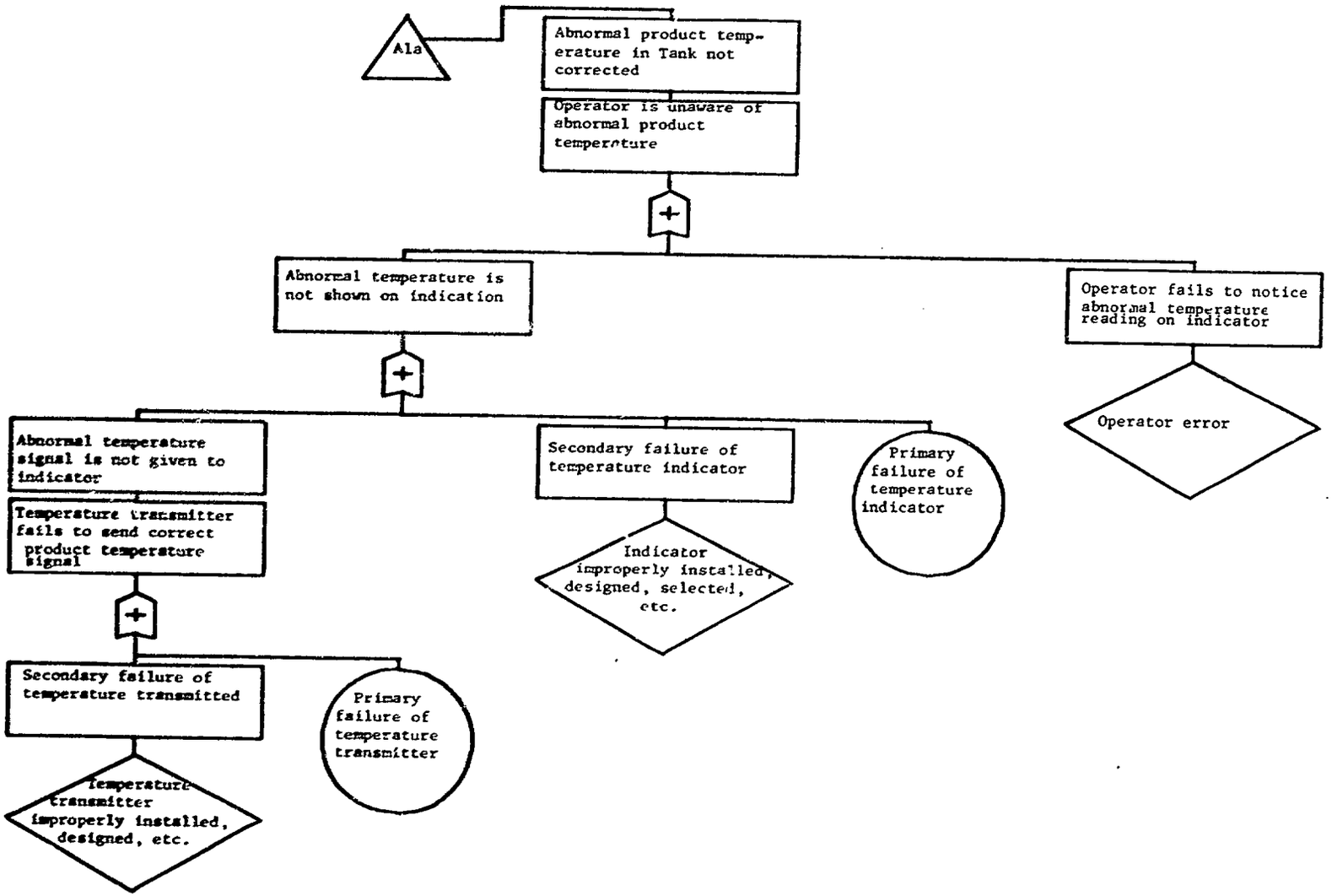

No product available From the Tank Farms
No product available to Tank Farms from 3" Transfer line
No product through Tank Farms
A
No product available to 3" Transfer line
No product from new pumphouse output flange
3" Transfer line fails to pass product
Product consumed by fire/ explosive in 3" Transfer line
C
D
No product available to output pumphouse flange connected to 3" Transfer line
No product from output line outside of new pumphouse
Flange connecting output line outside of new pumphouse with 3" Transfer line fails to pass product
Product consumed by fire/ explosion at flange connecting output line outside of new pumphouse with 3" Transfer line
E
F
No product available to output line outside of new pumphouse
Output line outside of new pumphouse fails to pass product
Product consumed by fire/ explosion in output line outside of new pumphouse
1
G
H

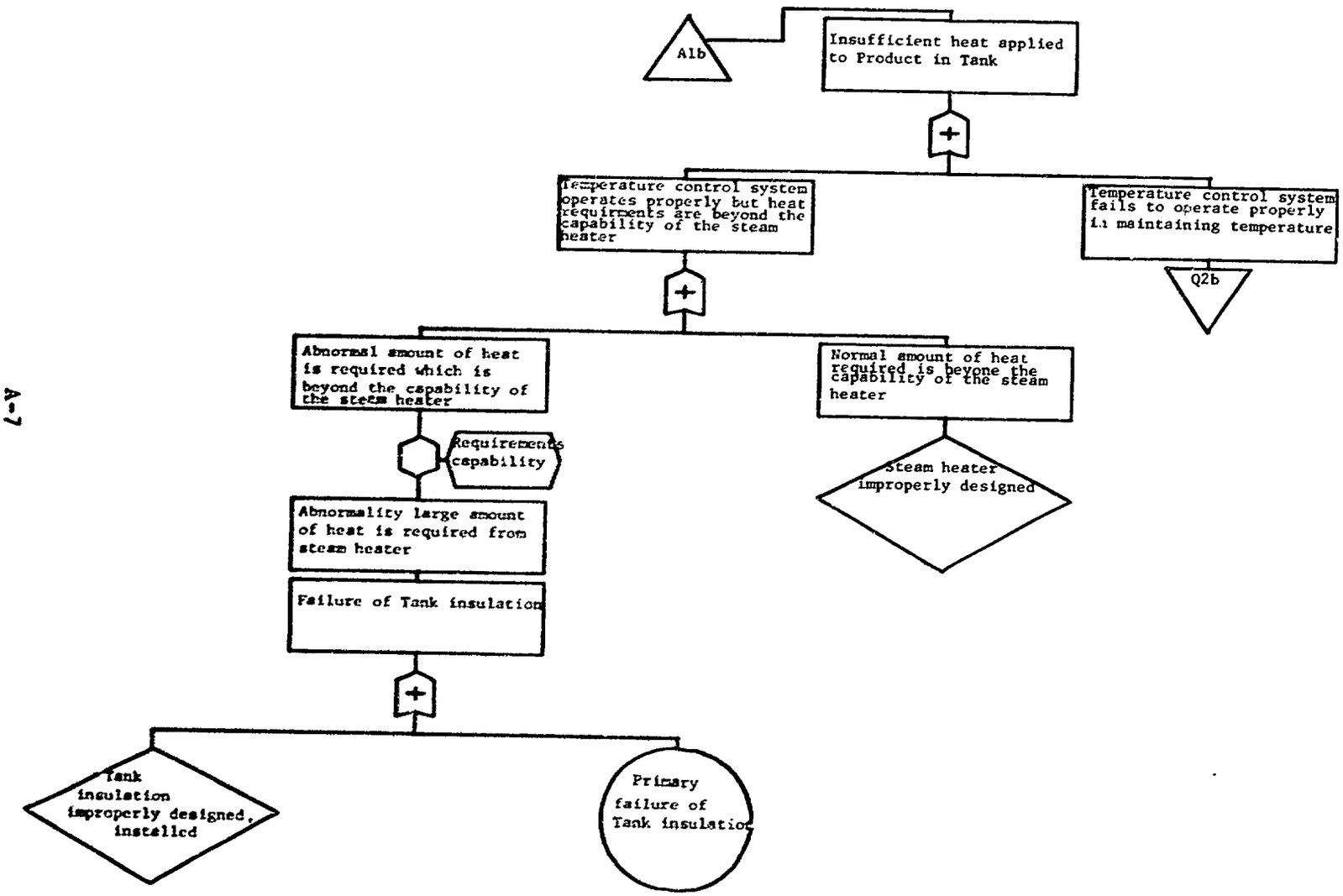

1
No product available to the output pipe outside of new pumphouse
No product from the output pipe inside new pumphouse
No product available to the output pipe inside the new pumphouse
No product from the two process pumps inside the new pumphouse
Final output pipe inside new pumpnouse fails to pass product
Product in output line inside new pumphouse consumed by fire/explosion
I
J
1-1
No product available to pumps
No product from pipe in new pump house which feeds pumps
Process pumps (and associated values) in new pumphouse fail to pass product
Product consumed by fire/ explosion in process pumps and associated values inside new pumphouse
K
L
No product available to pipes in new pumphouse which feed pumps
No product from pipeline between new pumphouse and storage tank
2
Pipe inside new pumphouse fails to pass product to pumps
M
Product in pipe inside new pumphouse which feed pumps is consumed by fire/explosive
N

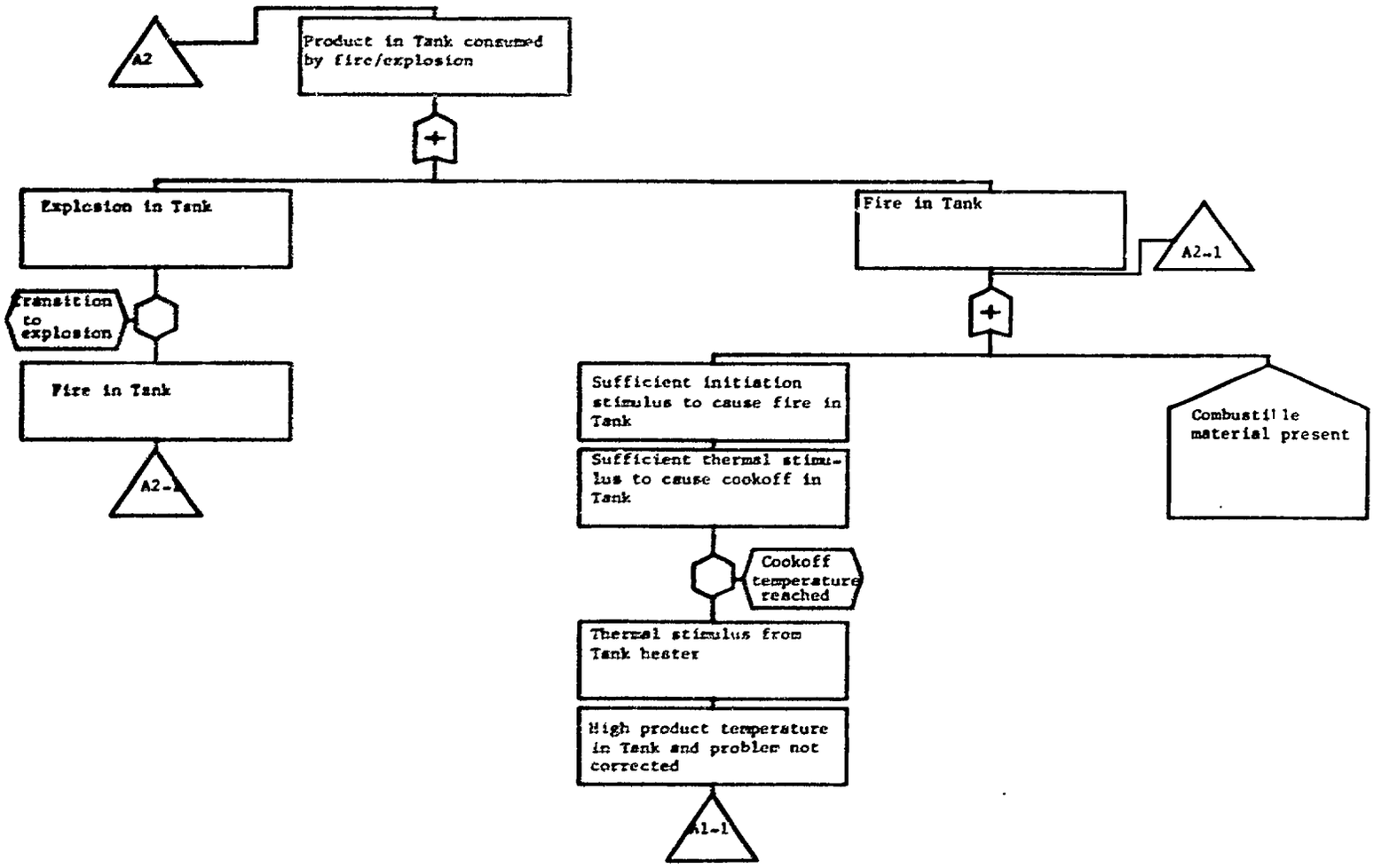

2
No product from pipeline between new pumphouse and storage tank
No product available to output pipe of Storage Tanks
No product from Storage Tank
Pipeline between new pumphouse and Storage Tank fails to pass product
Product consumed by fire/ explosive in pipeline between new pumphouse and Storage Tank
O
P
No product available to Storage Tank
No product from input Storage Tank pipes
New Storage Tank fails to pass product
Product consumed by fire/ explosion in Storage Tank
Q
R
No product available to input Storage Tank pipes
No product from pumps in Bldg 330 P-2
Pipe feeding new Storage Tank fails to pass product
Product consumed by fire/ explosion in pipe feeding Storage Tank
S
T
No product available to pumps in Bldg 330 P-2
Pumps in Bldg 330 P-2 fail to pass product
Product consumed by fire/ explosion in Bldg 330 P-2 pumps
U
V

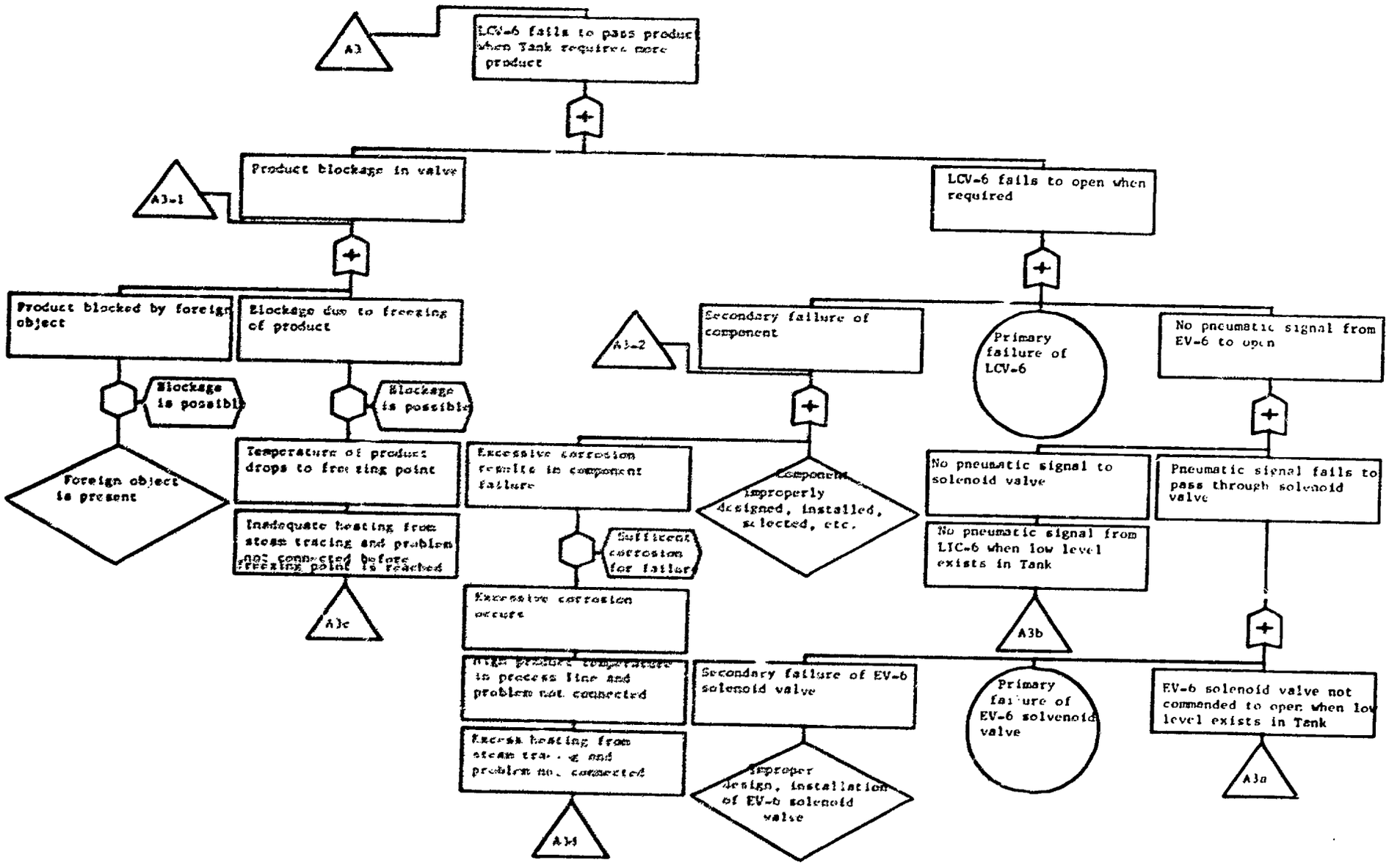

A
No product through Tank Farms
No product through C-3 Bldg
No product through one or more of the C-3 Tanks cause C-3 Bldg to be shutdown
No product through C-7 Bldg
No product through one or more of the C-7 Tank cause C-7 Bldg to be shut down
No product through 1st Tank of C-3
No product through 2nd Tank of C-3
No product through 3rd Tank of C-3
No product through 1st Tank of C-7
No product through 2nd Tank of C-7
No product through 3rd Tank of C-7
A-6
No product available to Tank
No product from LCV-6
Tank fails to pass product
Product in Tank consumed by fire/explosive
No product available to LCV-6
LCV-6 fails to pass product
Product at LCV-6 consumed by fire/explosive
A-5
A1
A2
A3
A4

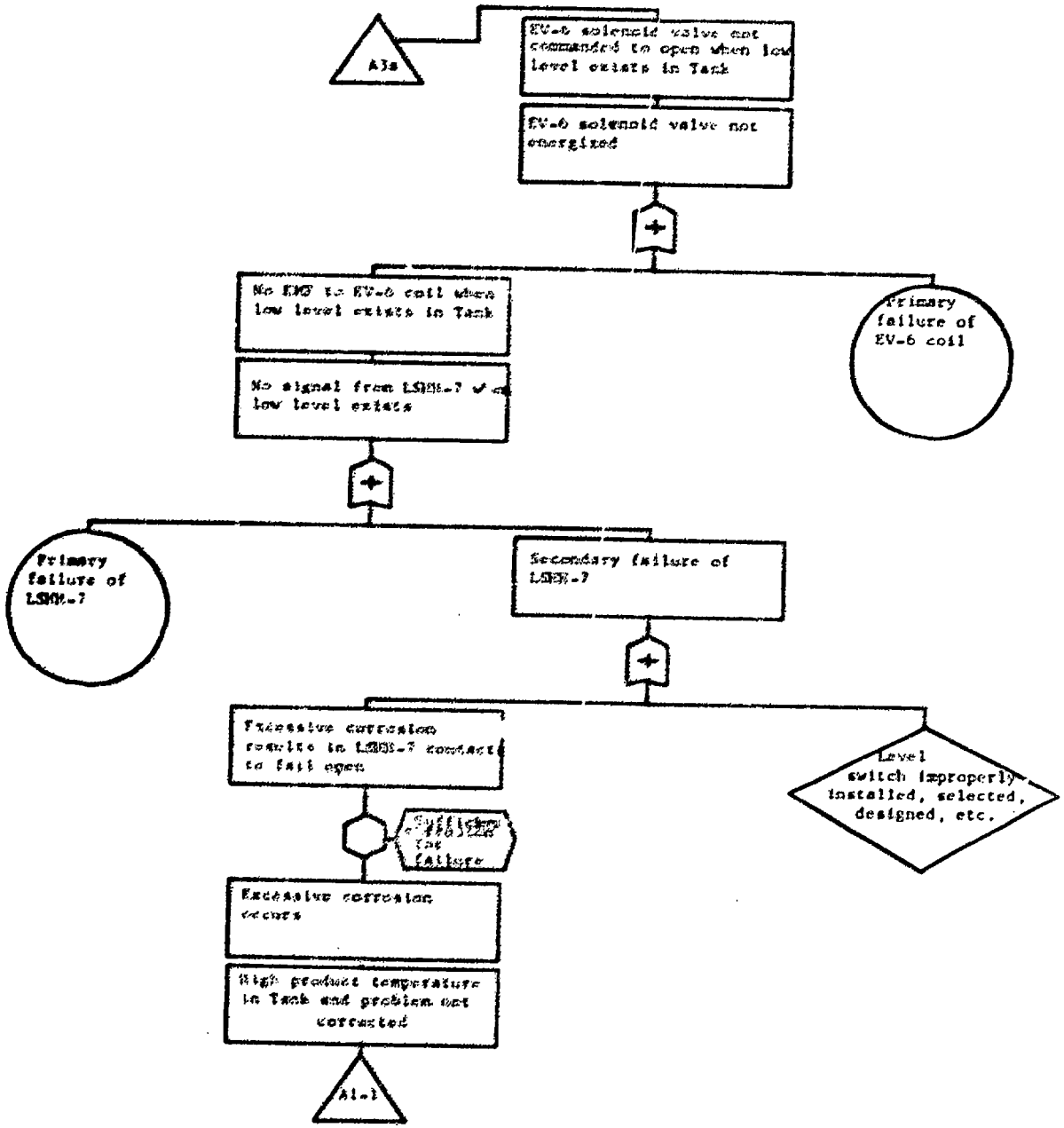

A1
Tank fails to pass product
Secondary failure of Tanks
Blockage in Tank
Primary failure of Tank
Product is frozen in Tank
Excessive corrosion results in tank failure
Tank improperly selected, installed, etc.
Blockage is possible
Sufficient corrosion for failure
Product temperature in Tank drops to freezing point before problem is corrected
Excessive corrosion occurs
A1-1
High product temperature in Tank and problem not connected
Temperature of product in Tanks drops
Product temperature not connected before freezing point is reached
Insufficient heat applied to product in Tank
Excessive heat applied to Tank
Abnormal product temperature in Tank not corrected
A1b
Abnormal product temperature not corrected
Freezing point will be reached if problem not corrected
Tempereture control syster fails to operate properly in maintaining product temperature
A1a
A1a
Q2b

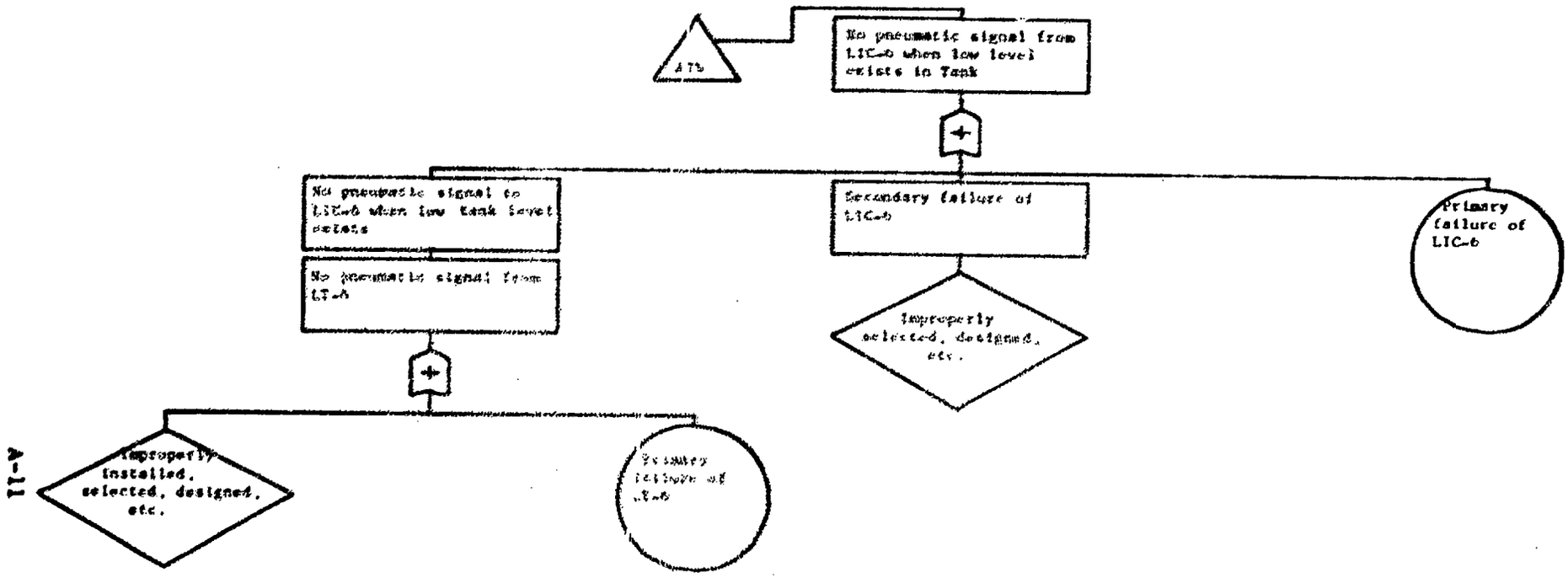

A1a
Abnormal product temperature in Tank not corrected
Operator is unaware of abnormal product temperature
Abnormal temperature is not shown on indication
Operator fails to notice abnormal temperature reading on indicator
Abnormal temperature signal is not given to indicator
Temperature transmitter fails to send correct product temperature signal
Secondary failure of temperature transmitted
Primary failure of temperature transmitter
Temperature transmitter improperly installed, designed, etc.
Secondary failure of temperature indicator
Primary failure of temperature indicator
Indicator improperly installed, designed, selected, etc.
Operator error

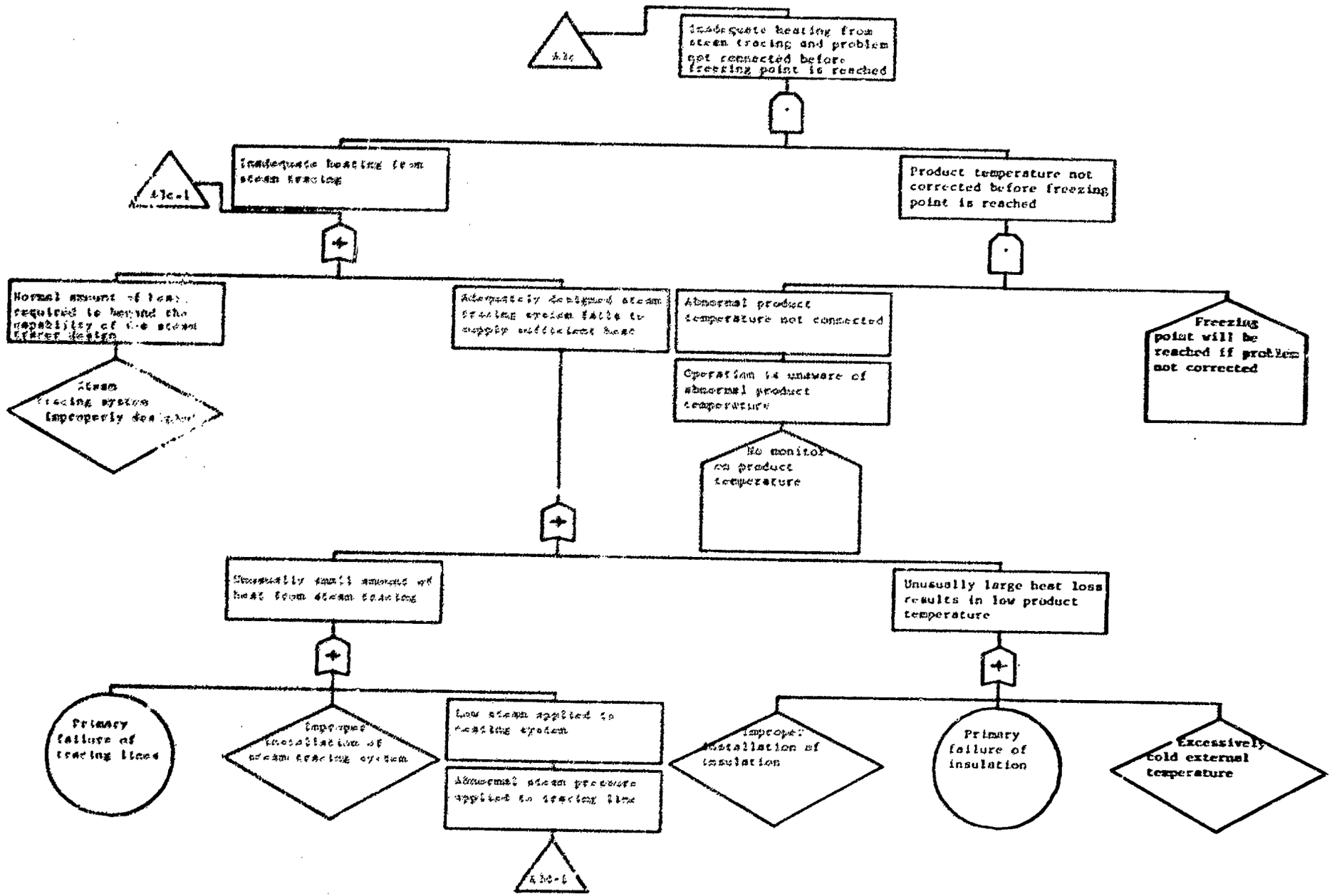

A1b
Insufficient heat applied to Product in Tank
Temperature control system operates properly but heat requirments are beyond the capability of the steam heater
Temperature control system fails to operate properly in maintaining temperature
Q2b
Abnormal amount of heat is required which is beyond the capability of the steam heater
Normal amount of heat required is beyone the capability of the steam heater
Requirements capability
Steam heater improperly designed
Abnormality large amount of heat is required from steam heater
Failure of Tank insulation
Tank insulation improperly designed, installed
Primary failure of Tank insulatio

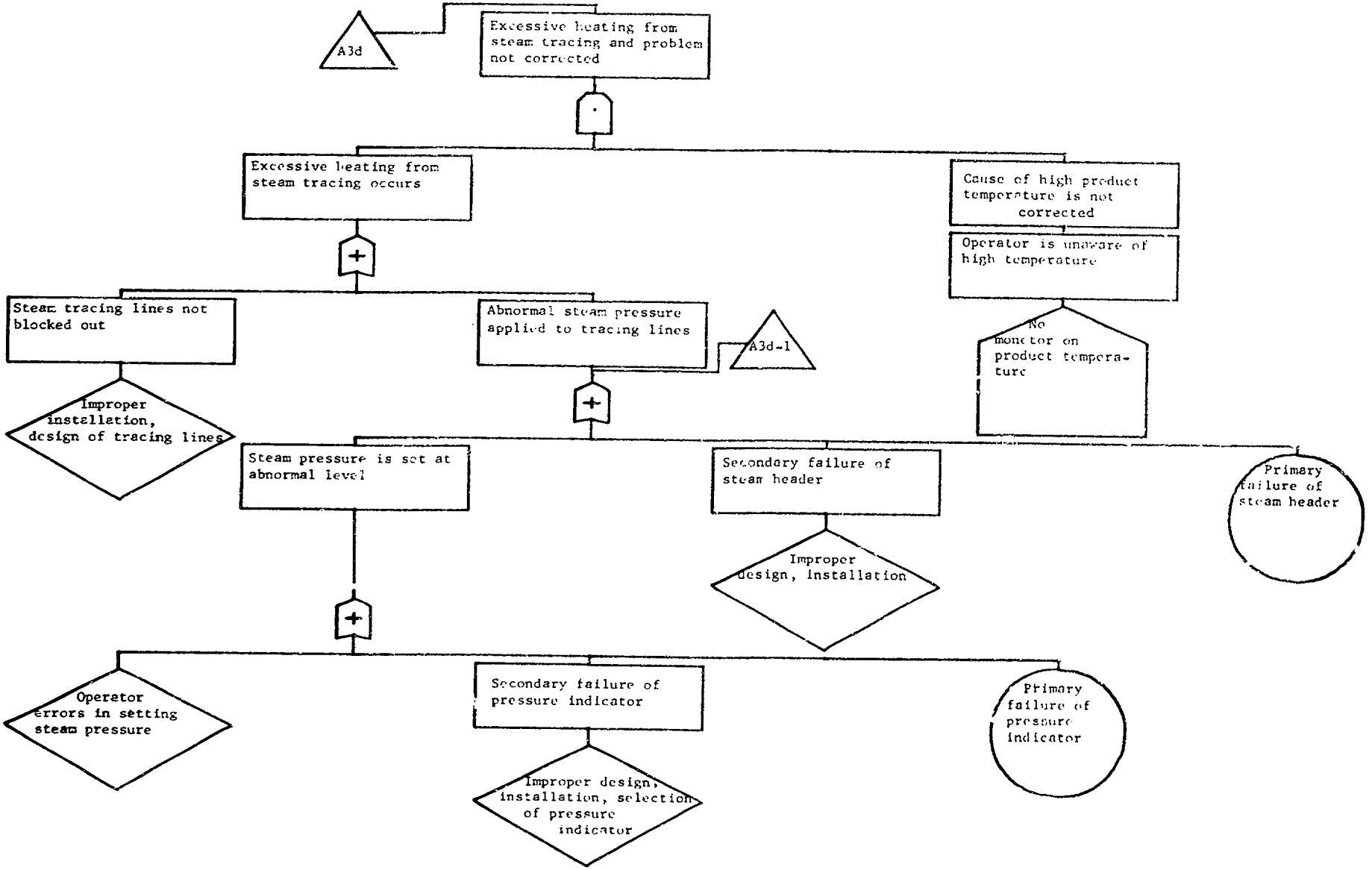

A2
Product in Tank consumed by fire/explosion
Explosion in Tank
Transition to explosion
Fire in Tank
A2-1
Fire in Tank
A2-1
Sufficient initiation stimulus to cause fire in Tank
Sufficient thermal stimulus to cause cookoff in Tank
Cookoff temperature reached
Thermal stimulus from Tank heater
High product temperature in Tank and problem not corrected
A1-1
Combustible material present

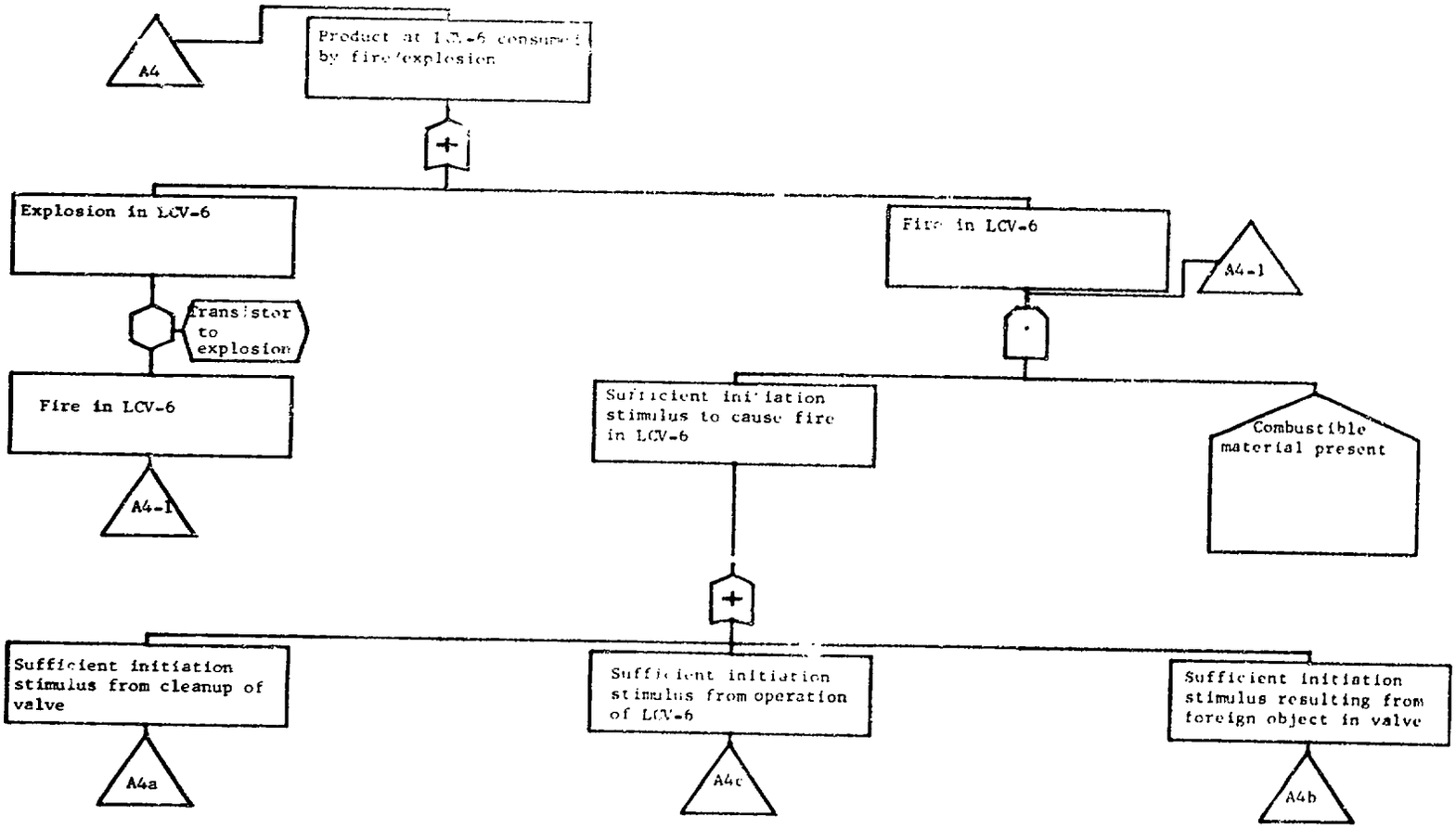

A3
LCV-6 fails to pass product when Tank requires more product
A3-1
Product blockage in valve
LCV-6 fails to open when required
Product blocked by foreign object
Blockage due to freezing of product
A3-2
Secondary failure of component
Primary failure of LCV-6
No pneumatic signal from EV-6 to open
Blockage is possible
Blockage is possible
Foreign object is present
Temperature of product drops to freezing point
Excessive corrosion results in component failure
Component improperly designed, installed, selected, etc.
No pneumatic signal to solenoid valve
Pneumatic signal fails to pass through solenoid valve
Inadequate heating from steam tracing and problem not connected before freezing point is reached
Sufficient corrosion for failure
No pneumatic signal from LIC-6 when low level exists in Tank
A3c
Excessive corrosion occurs
A3b
High product temperature in process line and problem not connected
Secondary failure of EV-6 solenoid valve
Primary failure of EV-6 solvenoid valve
EV-6 solenoid valve not commanded to open when low level exists in Tank
Excess heating from steam tra. . g and problem no. connected
Improper design, installation of EV-6 solenoid valve
A3a
A3d

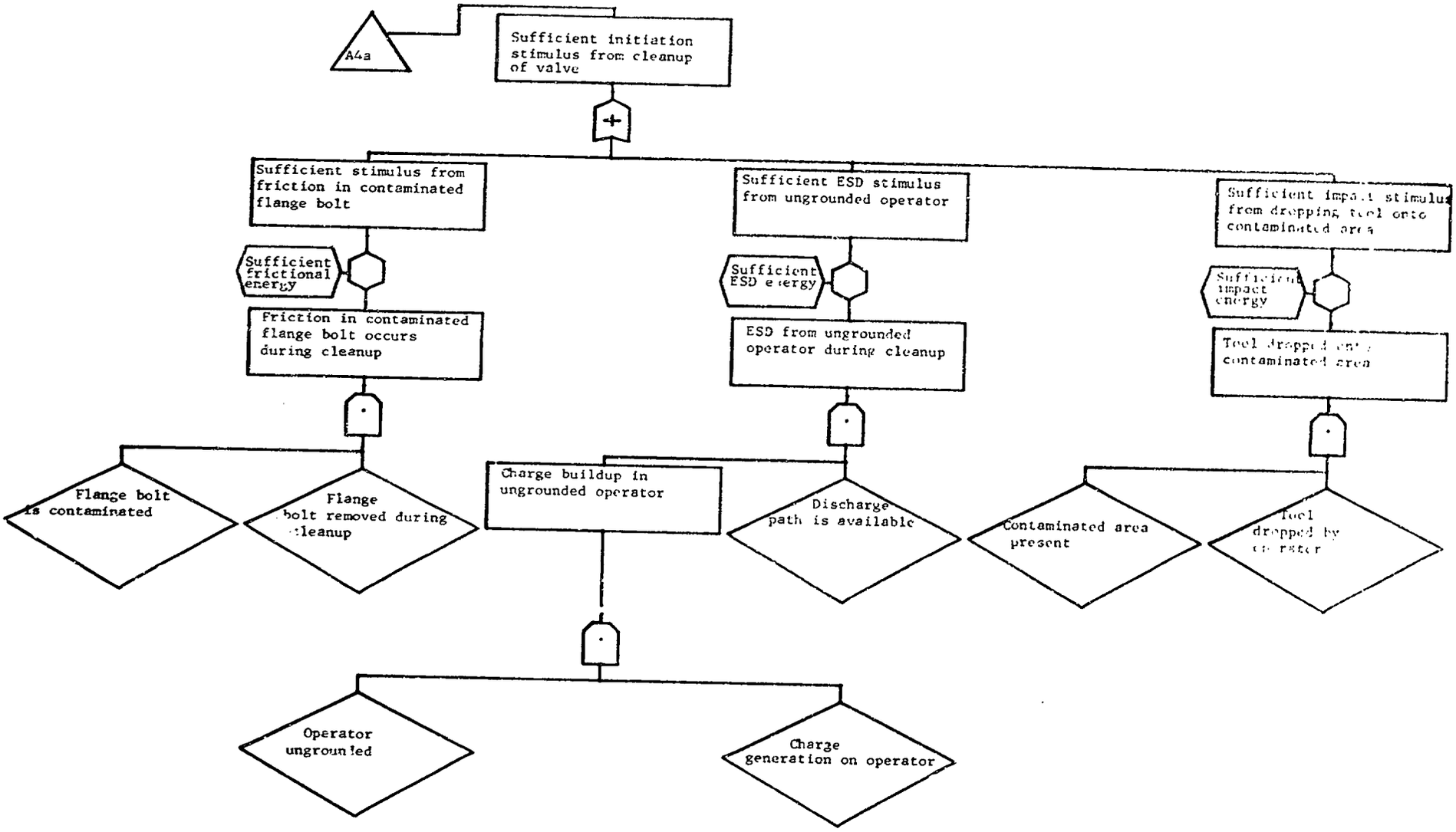

A3a
EV-6 solenoid valve not commanded to open when low level exists in Tank
EV-6 solenoid valve not energized
No EMF to EV-6 coil when low level exists in Tank
No signal from LSHL-7 when low level exists
Primary failure of EV-6 coil
Primary failure of LSHL-7
Secondary failure of LSHL-7
Excessive corrosion results in LSHL-7 contacts to fail open
Sufficient time for failure
Excessive corrosion occurs
High product temperature in Tank and problem not corrected
A1-1
Level switch improperly installed, selected, designed, etc.

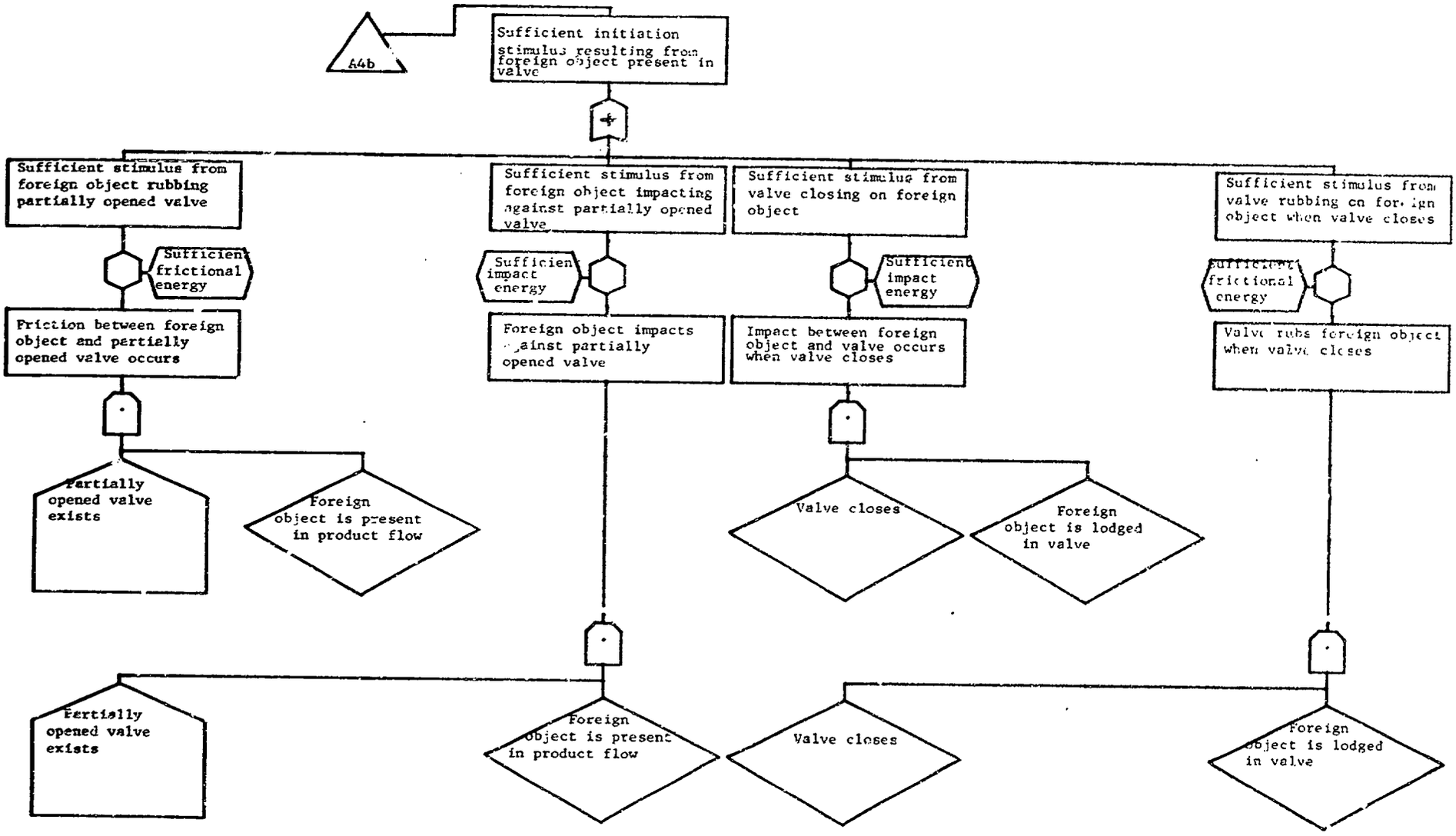

No pneumatic signal from LIC-6 when low level exists in Tank
No pneumatic signal to LIC-6 when low tank level exists
No pneumatic signal from LT-6
Improperly installed, selected, designed, etc.
Secondary failure of LIC-6
Improperly selected, designed, etc.
Primary failure of LIC-6

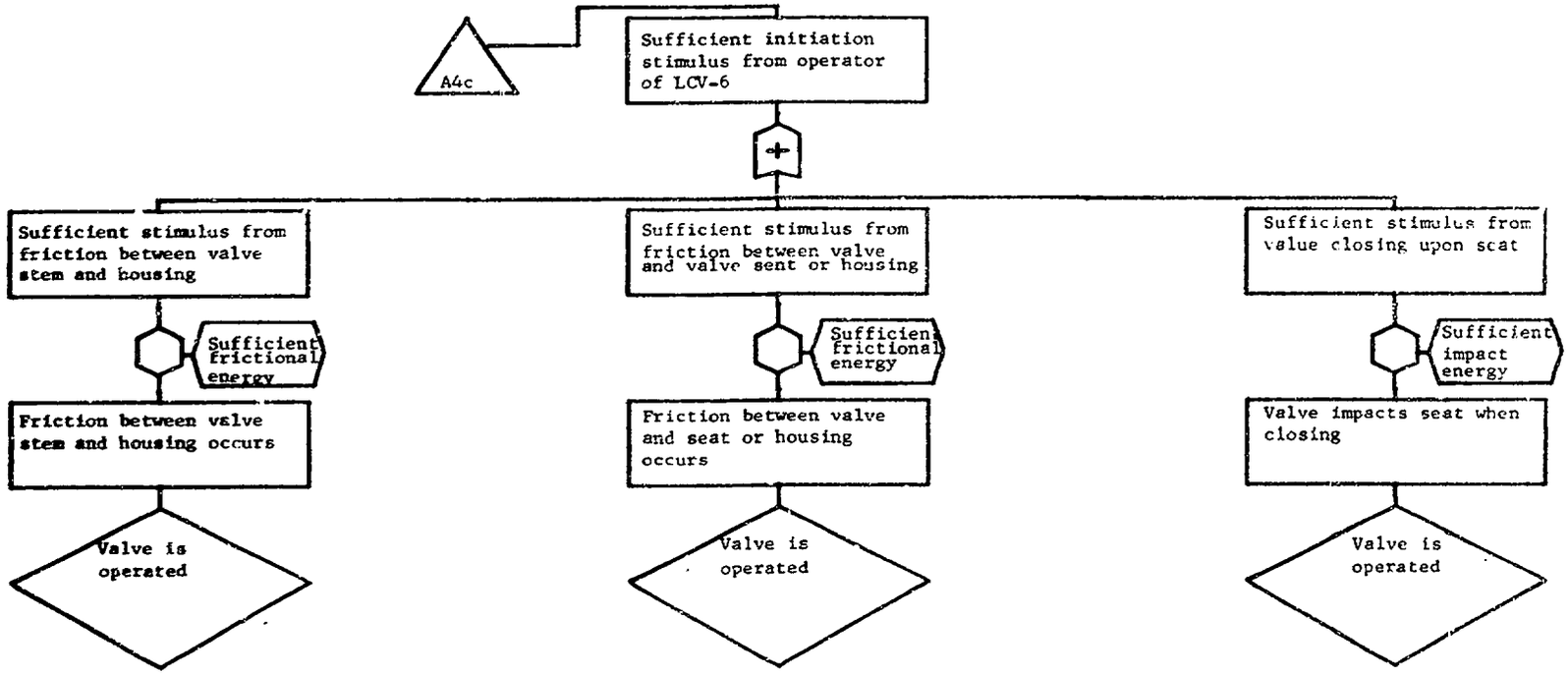

A2c
Inadequate heating from steam tracing and problem not corrected before freezing point is reached
A2c-1
Inadequate heating from steam tracing
Product temperature not corrected before freezing point is reached
Normal amount of heat required to be in the capability of the steam tracer design
Steam tracing system improperly designed
Inadequately designed steam tracing system fails to supply sufficient heat
Abnormal product temperature not corrected
Operation is unaware of abnormal product temperature
No monitor on product temperature
Freezing point will be reached if problem not corrected
Unusually small amount of heat from steam tracing
Unusually large heat loss results in low product temperature
Primary failure of tracing lines
Improper installation of steam tracing system
Low steam applied to tracing system
Abnormal steam pressure applied to tracing line
A2c-2
Improper installation of insulation
Primary failure of insulation
Excessively cold external temperature

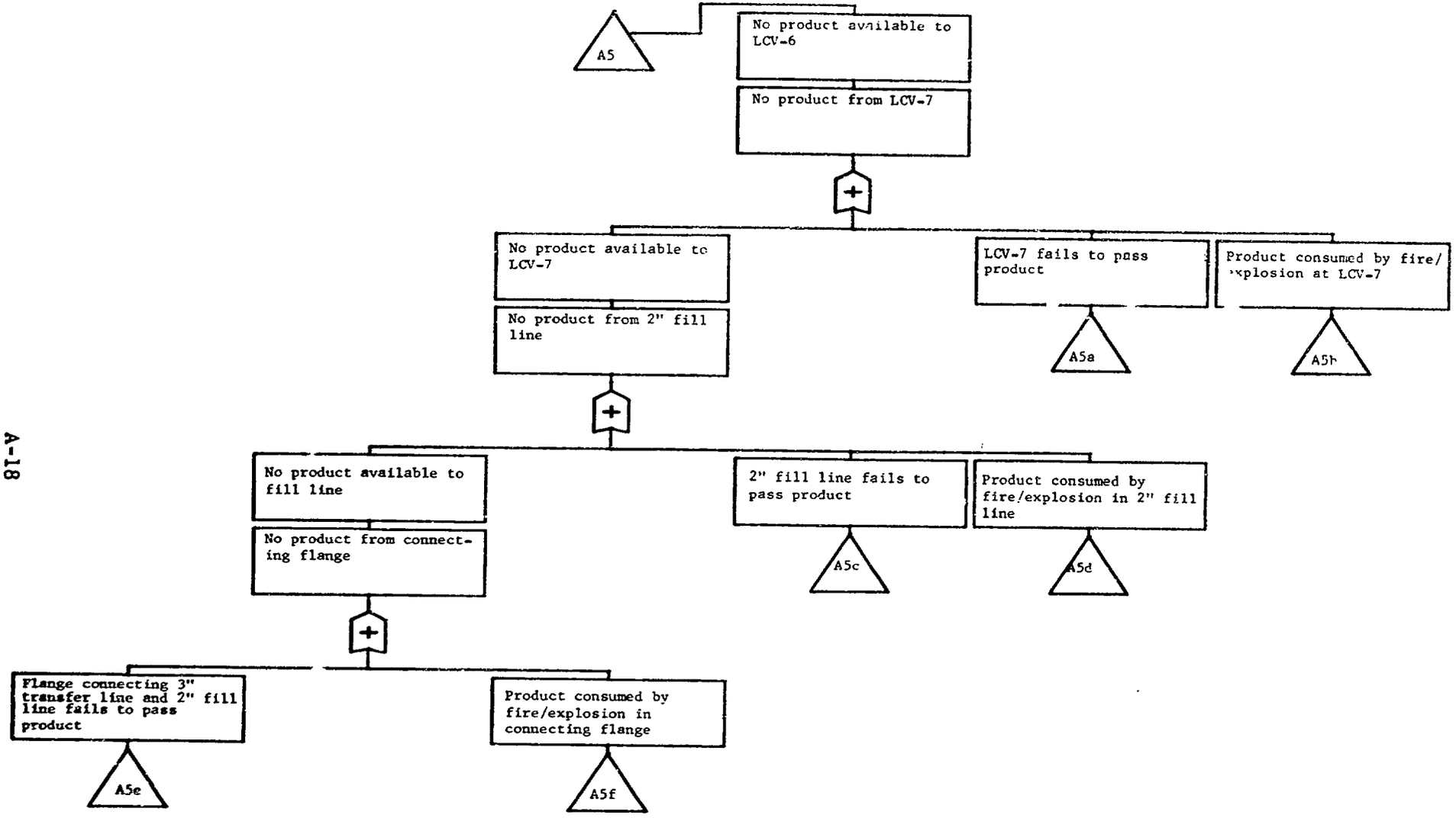

A3d
Excessive heating from steam tracing and problem not corrected
Excessive heating from steam tracing occurs
Cause of high product temperature is not corrected
Operator is unaware of high temperature
No monitor on product temperature
Steam tracing lines not blocked out
Improper installation, design of tracing lines
Abnormal steam pressure applied to tracing lines
A3d-1
Steam pressure is set at abnormal level
Secondary failure of steam header
Improper design, installation
Primary failure of steam header
Operator errors in setting steam pressure
Secondary failure of pressure indicator
Improper design, installation, selection of pressure indicator
Primary failure of pressure indicator

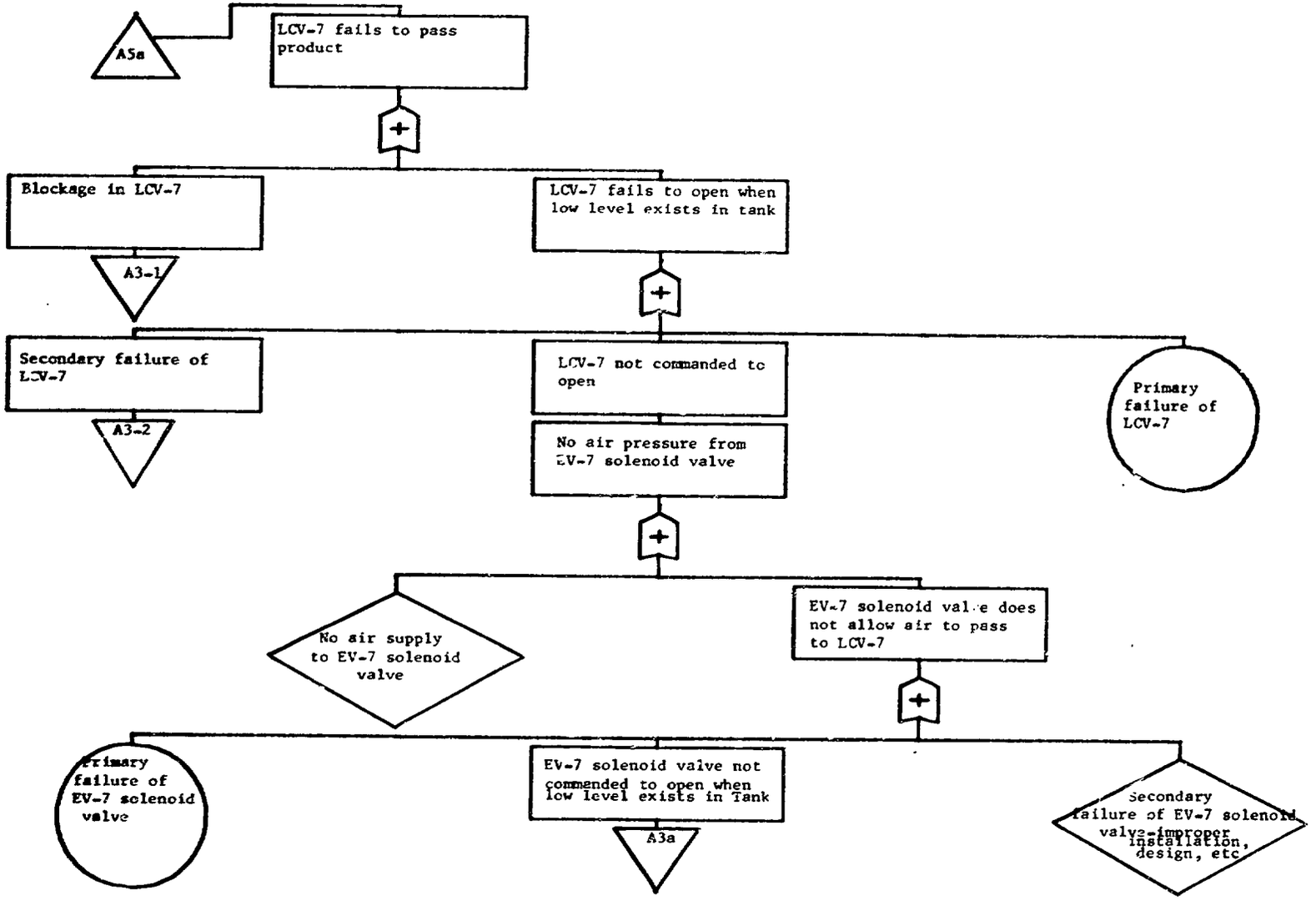

A4
Product at LCV-6 consumed by fire/explosion
Explosion in LCV-6
Transistor to explosion
Fire in LCV-6
A4-1
Fire in LCV-6
A4-1
Sufficient initiation stimulus to cause fire in LCV-6
Combustible material present
Sufficient initiation stimulus from cleanup of valve
A4a
Sufficient initiation stimulus from operation of LCV-6
A4c
Sufficient initiation stimulus resulting from foreign object in valve
A4b

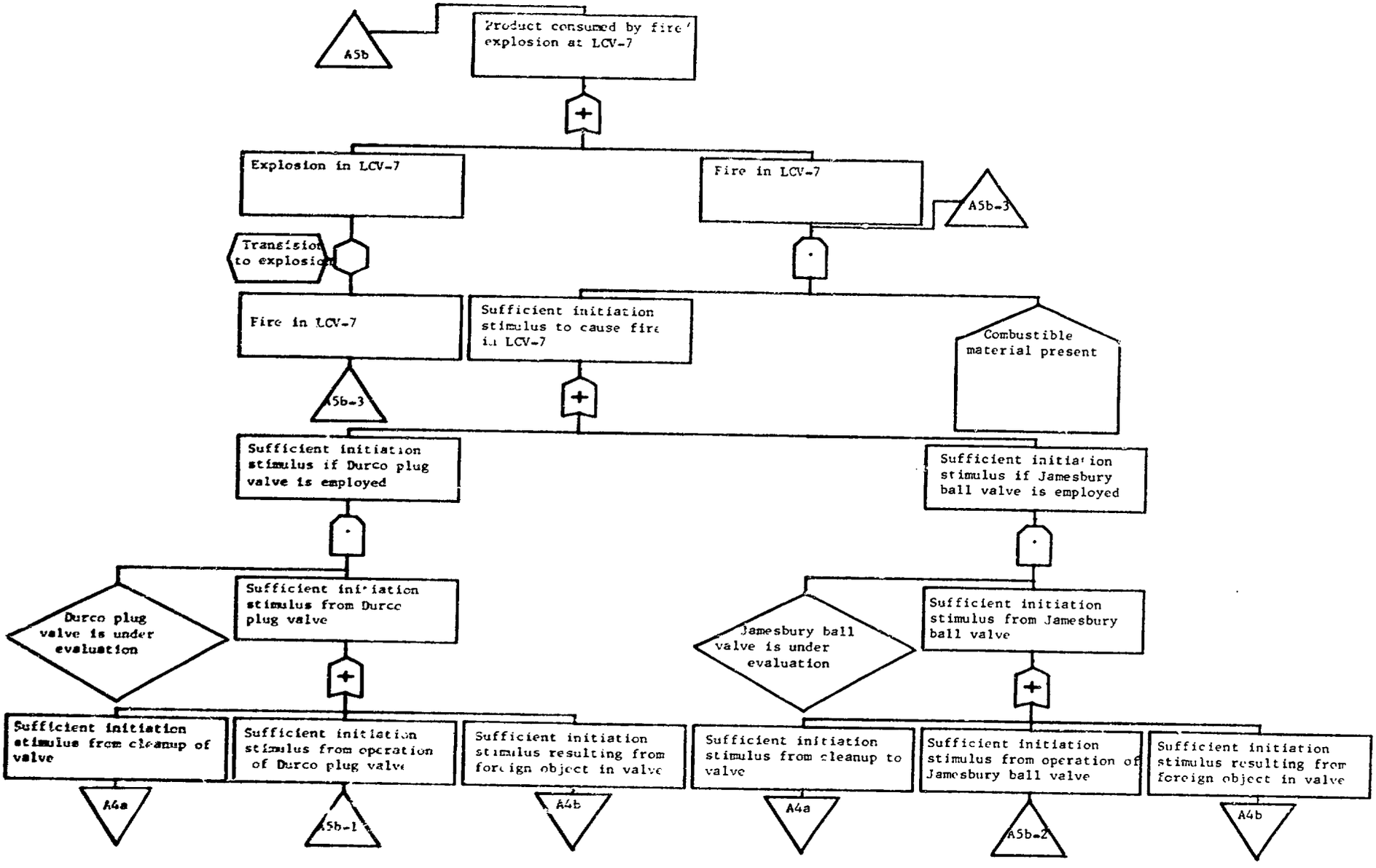

A4a
Sufficient initiation stimulus from cleanup of valve
+
Sufficient stimulus from friction in contaminated flange bolt
Sufficient ESD stimulus from ungrounded operator
Sufficient impact stimulus from dropping tool onto contaminated area
Sufficient frictional energy
Sufficient ESD energy
Sufficient impact energy
Friction in contaminated flange bolt occurs during cleanup
ESD from ungrounded operator during cleanup
Tool dropped onto contaminated area
Flange bolt is contaminated
Flange bolt removed during cleanup
Charge buildup in ungrounded operator
Discharge path is available
Contaminated area present
Tool dropped by operator
Operator ungrounded
Charge generation on operator

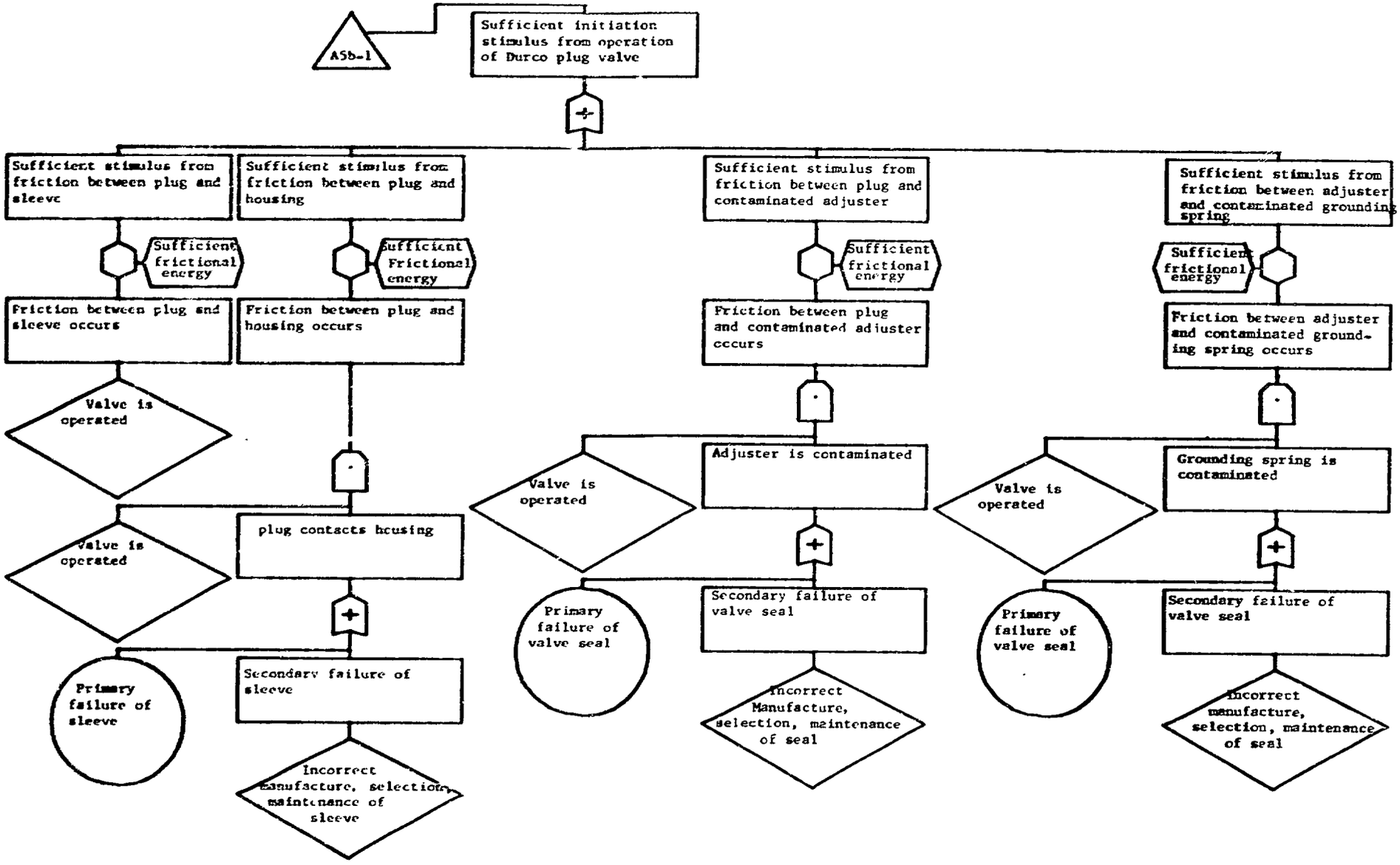

A4b
Sufficient initiation stimulus resulting from foreign object present in valve
Sufficient stimulus from foreign object rubbing partially opened valve
Sufficient frictional energy
Friction between foreign object and partially opened valve occurs
Partially opened valve exists
Foreign object is present in product flow
Sufficient stimulus from foreign object impacting against partially opened valve
Sufficient impact energy
Foreign object impacts against partially opened valve
Sufficient stimulus from valve closing on foreign object
Sufficient impact energy
Impact between foreign object and valve occurs when valve closes
Valve closes
Foreign object is lodged in valve
Sufficient stimulus from valve rubbing on foreign object when valve closes
Sufficient frictional energy
Valve rubs foreign object when valve closes
Partially opened valve exists
Foreign object is present in product flow
Valve closes
Foreign object is lodged in valve

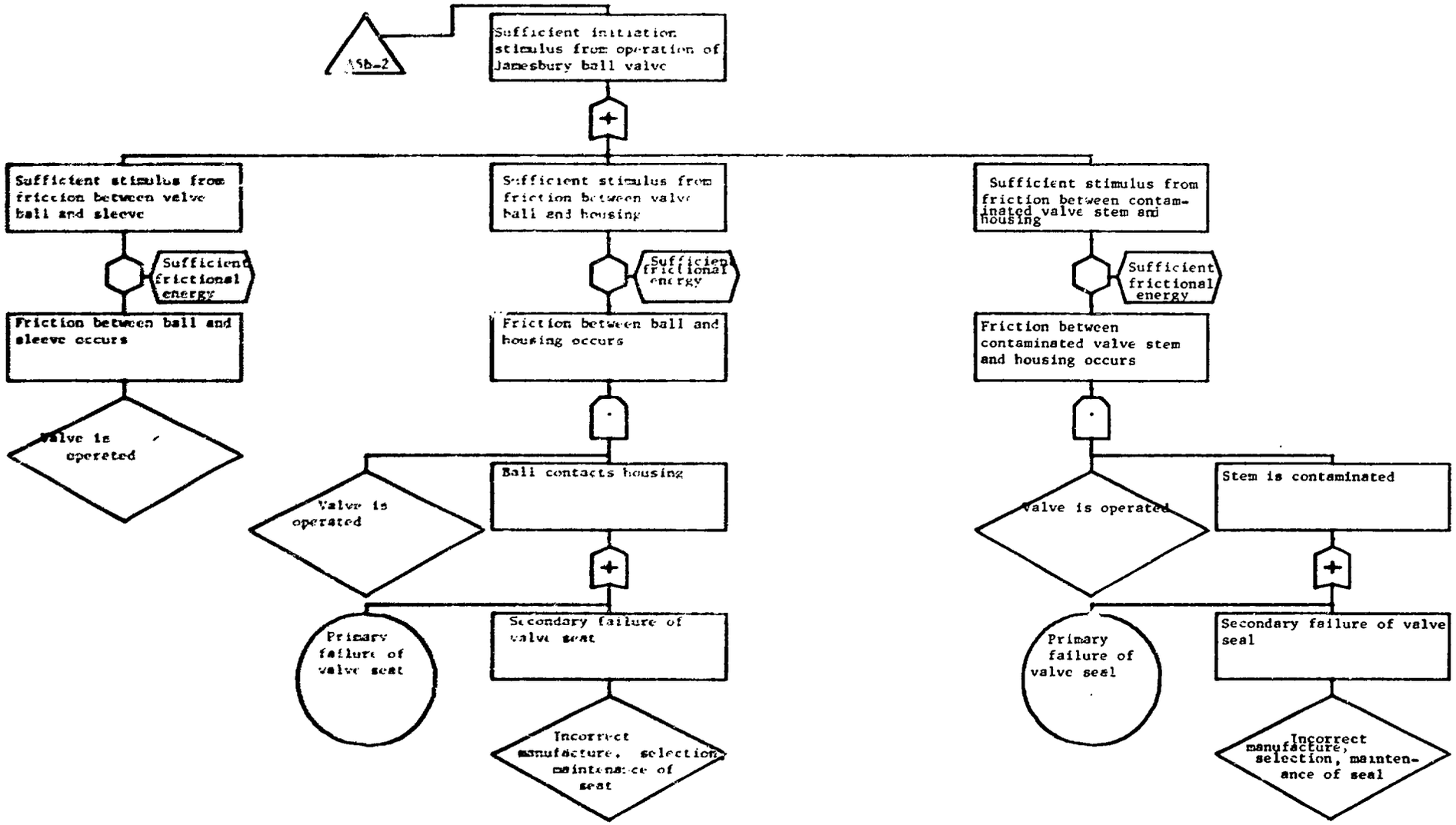

A4c
Sufficient initiation stimulus from operator of LCV-6
Sufficient stimulus from friction between valve stem and housing
Sufficient frictional energy
Friction between valve stem and housing occurs
Valve is operated
Sufficient stimulus from friction between valve and valve sent or housing
Sufficient frictional energy
Friction between valve and seat or housing occurs
Valve is operated
Sufficient stimulus from value closing upon seat
Sufficient impact energy
Valve impacts seat when closing
Valve is operated

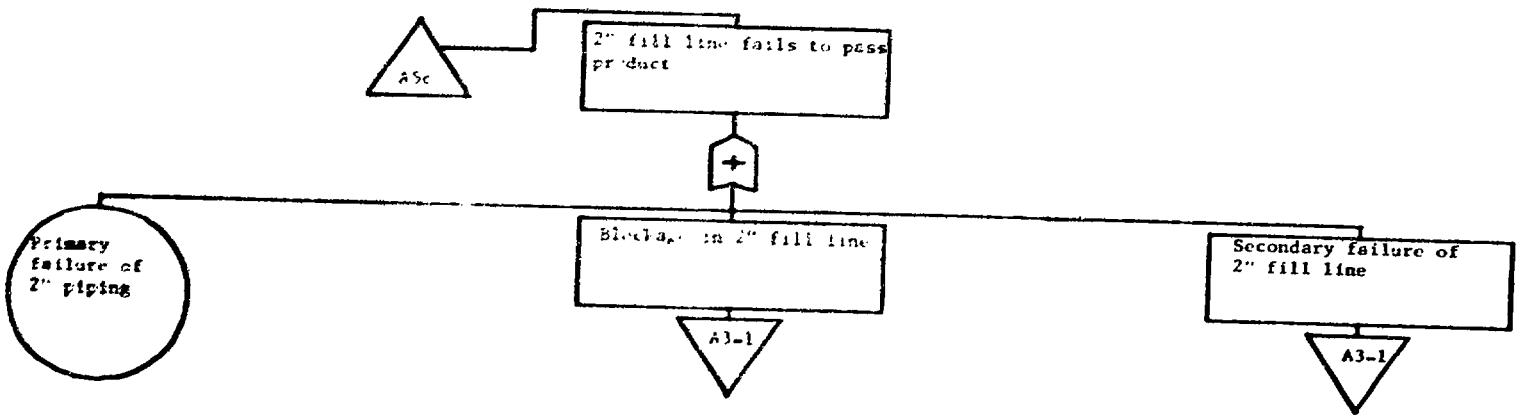

A5
No product available to LCV-6
No product from LCV-7
No product available to LCV-7
No product from 2" fill line
LCV-7 fails to pass product
Product consumed by fire/explosion at LCV-7
A5a
A5b
No product available to fill line
No product from connecting flange
2" fill line fails to pass product
Product consumed by fire/explosion in 2" fill line
A5c
A5d
Flange connecting 3" transfer line and 2" fill line fails to pass product
Product consumed by fire/explosion in connecting flange
A5e
A5f

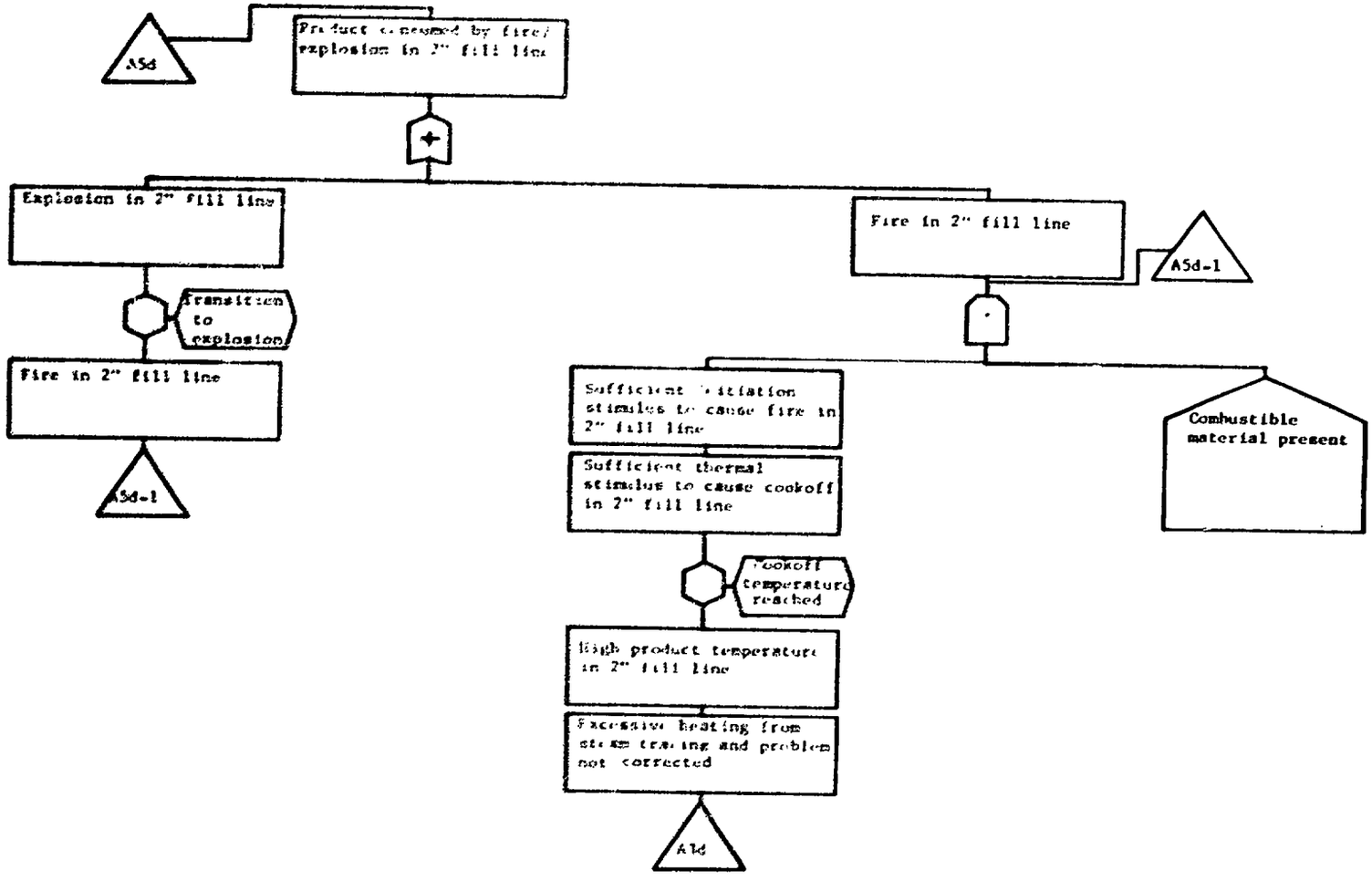

A5a
LCV-7 fails to pass product
Blockage in LCV-7
LCV-7 fails to open when low level exists in tank
A3-1
Secondary failure of LCV-7
A3-2
LCV-7 not commanded to open
No air pressure from EV-7 solenoid valve
Primary failure of LCV-7
No air supply to EV-7 solenoid valve
EV-7 solenoid valve does not allow air to pass to LCV-7
Primary failure of EV-7 solenoid valve
EV-7 solenoid valve not commended to open when low level exists in Tank
A3a
Secondary failure of EV-7 solenoid valve-improper installation, design, etc

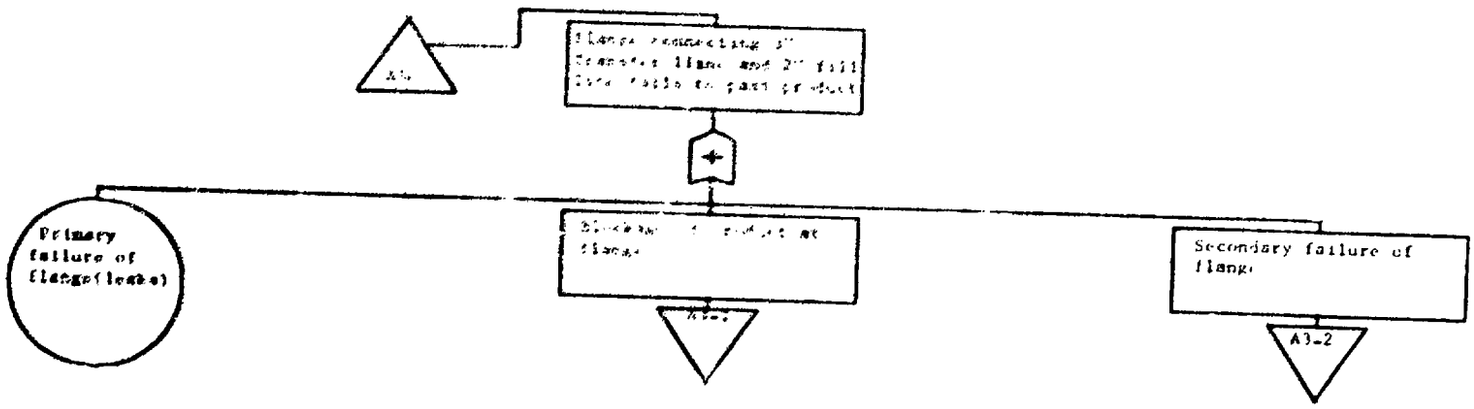

A5b
Product consumed by fire/explosion at LCV-7
Explosion in LCV-7
Fire in LCV-7
A5b-3
Transition to explosion
Fire in LCV-7
Sufficient initiation stimulus to cause fire in LCV-7
Combustible material present
A5b-3
Sufficient initiation stimulus if Durco plug valve is employed
Sufficient initiation stimulus if Jamesbury ball valve is employed
Durco plug valve is under evaluation
Sufficient initiation stimulus from Durco plug valve
Jamesbury ball valve is under evaluation
Sufficient initiation stimulus from Jamesbury ball valve
Sufficient initiation stimulus from cleanup of valve
Sufficient initiation stimulus from operation of Durco plug valve
Sufficient initiation stimulus resulting from foreign object in valve
Sufficient initiation stimulus from cleanup to valve
Sufficient initiation stimulus from operation of Jamesbury ball valve
Sufficient initiation stimulus resulting from foreign object in valve
A4a
A5b-1
A4b
A4a
A5b-2
A4b

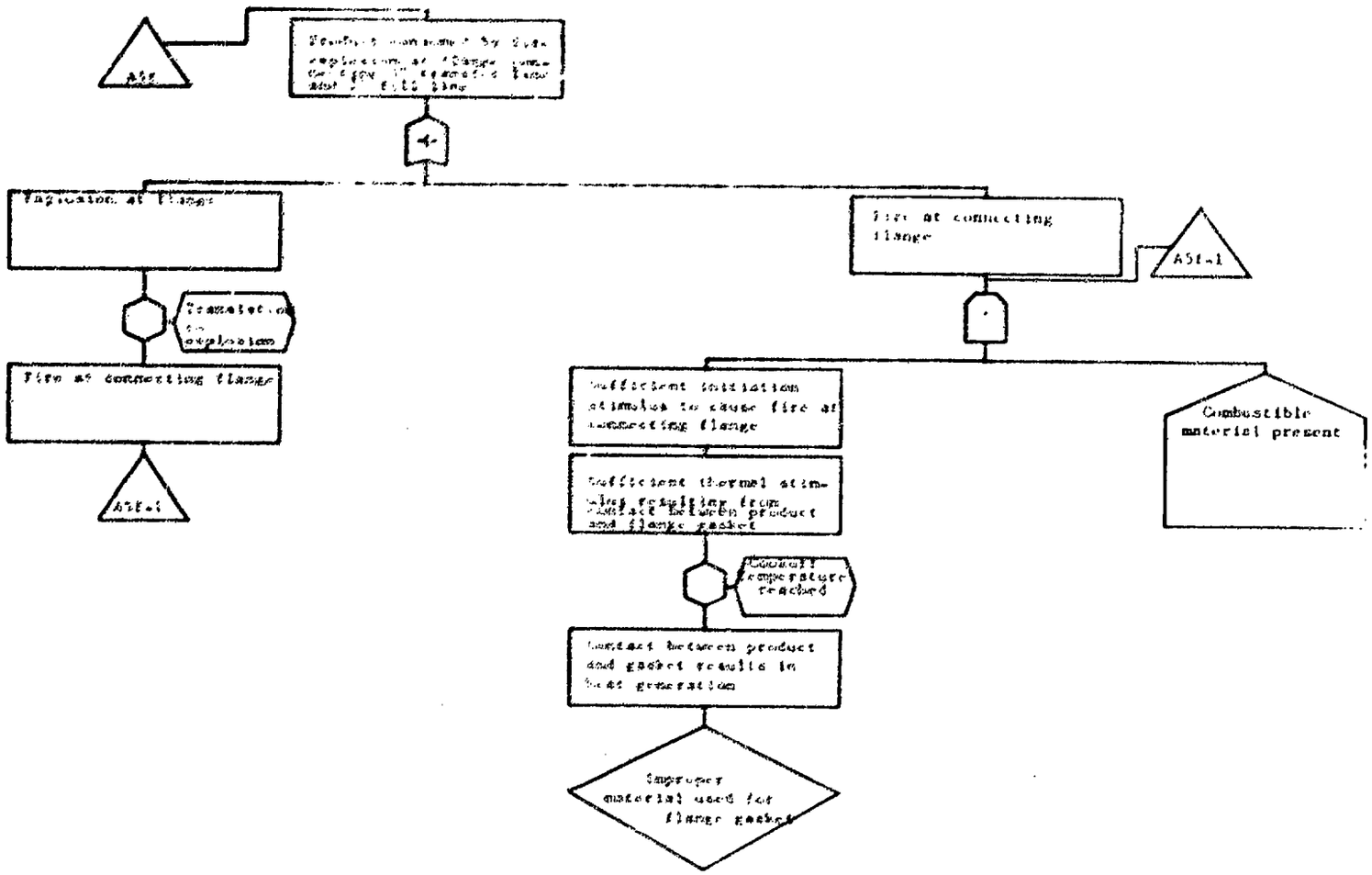

A5b-1
Sufficient initiation stimulus from operation of Durco plug valve
Sufficient stimulus from friction between plug and sleeve
Sufficient stimulus from friction between plug and housing
Sufficient stimulus from friction between plug and contaminated adjuster
Sufficient stimulus from friction between adjuster and contaminated grounding spring
Sufficient frictional energy
Sufficient Frictional energy
Sufficient frictional energy
Sufficient frictional energy
Friction between plug and sleeve occurs
Friction between plug and housing occurs
Friction between plug and contaminated adjuster occurs
Friction between adjuster and contaminated grounding spring occurs
Valve is operated
Valve is operated
plug contacts housing
Valve is operated
Valve is operated
Adjuster is contaminated
Grounding spring is contaminated
Primary failure of sleeve
Secondary failure of sleeve
Incorrect Manufacture, selection, maintenance of sleeve
Primary failure of valve seal
Secondary failure of valve seal
Incorrect Manufacture, selection, maintenance of seal
Primary failure of valve seal
Secondary failure of valve seal
Incorrect manufacture, selection, maintenance of seal

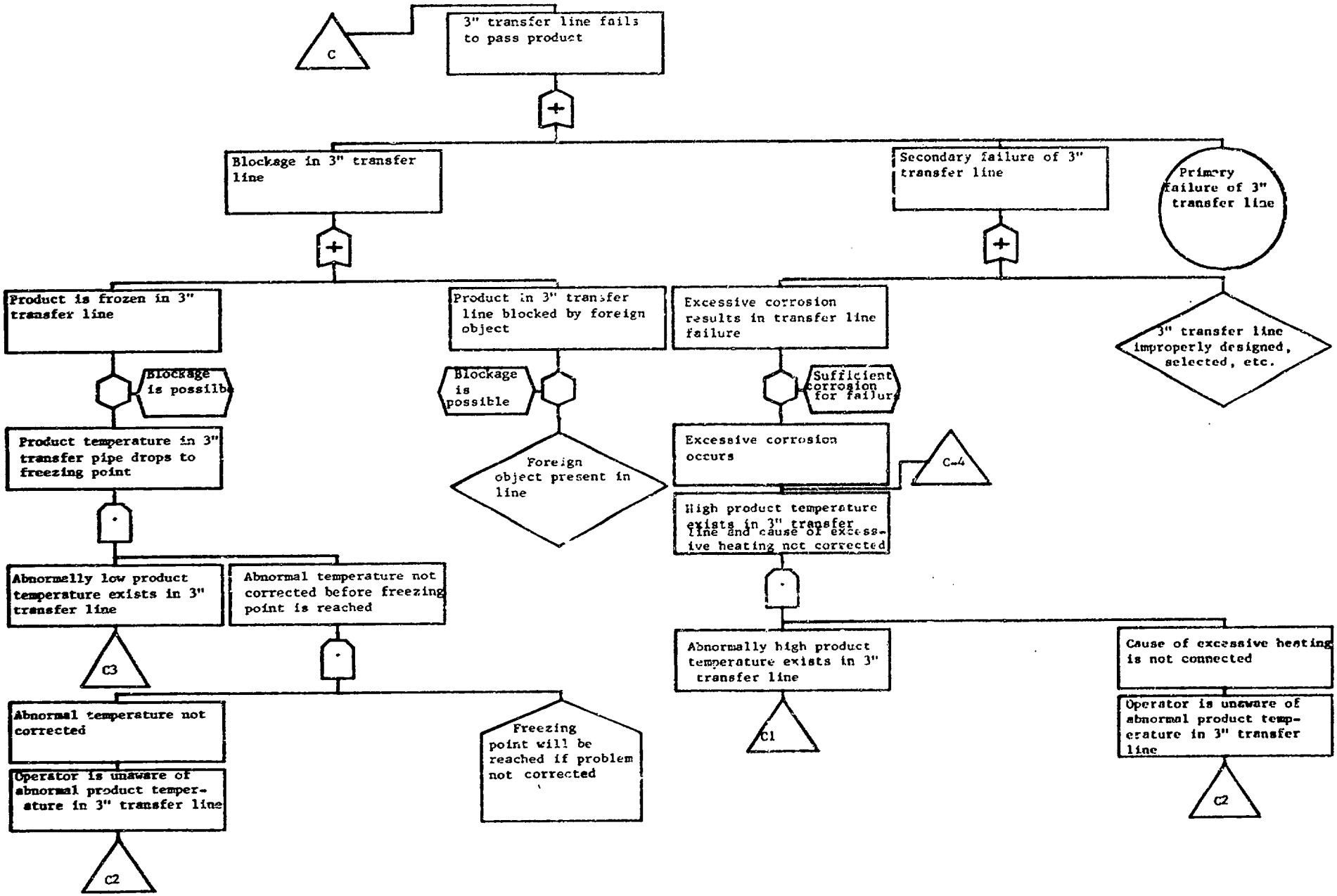

Sb-2
Sufficient initiation stimulus from operation of Jamesbury ball valve
Sufficient stimulus from friction between valve ball and sleeve
Sufficient frictional energy
Friction between ball and sleeve occurs
Valve is opereted
Sufficient stimulus from friction between valve ball and housing
Sufficient frictional energy
Friction between ball and housing occurs
Valve is operated
Ball contacts housing
Primary failure of valve seat
Secondary failure of valve seat
Incorrect manufacture, selection, maintenance of seat
Sufficient stimulus from friction between contaminated valve stem and housing
Sufficient frictional energy
Friction between contaminated valve stem and housing occurs
Valve is operated
Stem is contaminated
Primary failure of valve seal
Secondary failure of valve seal
Incorrect manufacture, selection, maintenance of seal

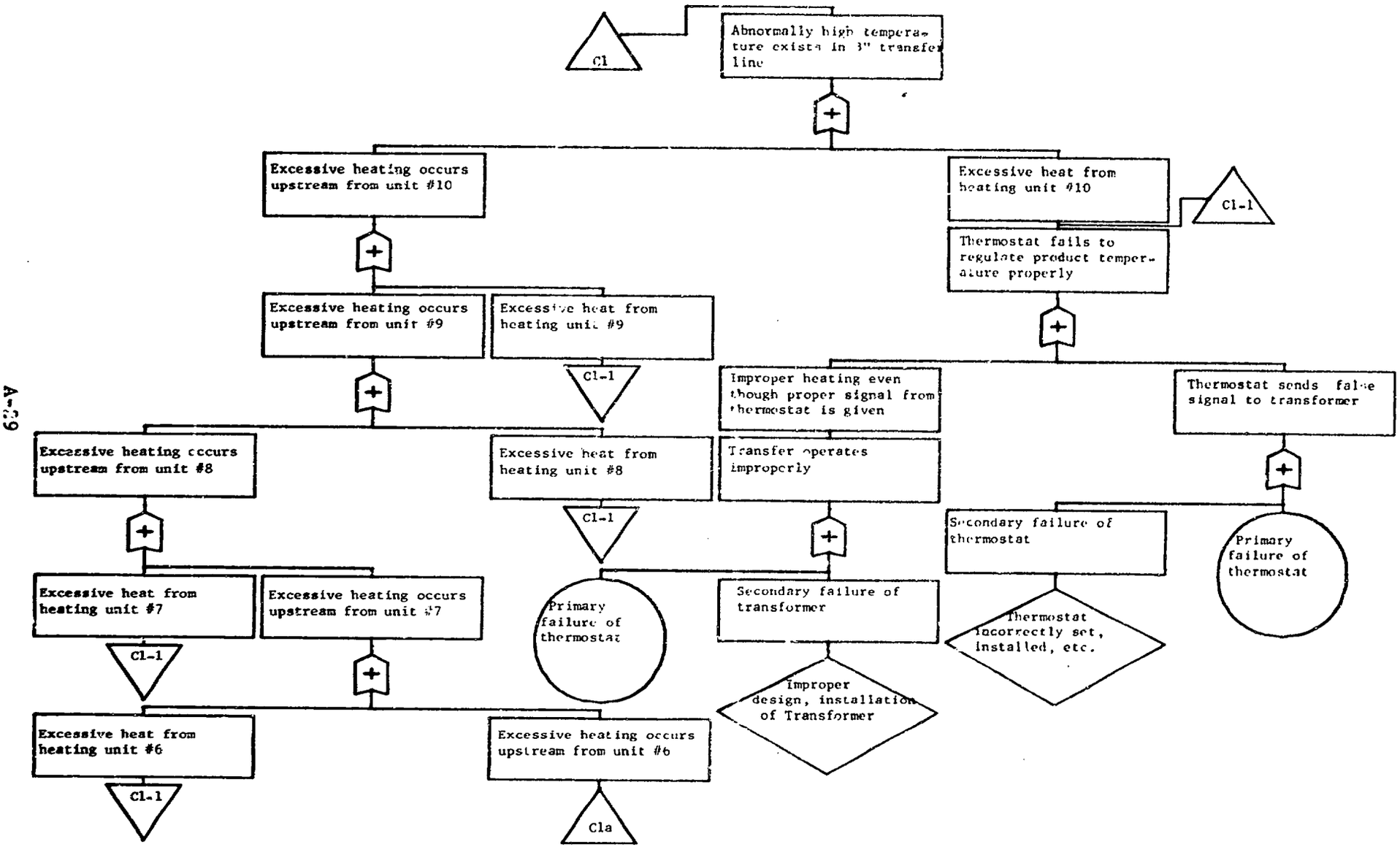

A5c
2" fill line fails to pass product
Primary failure of 2" piping
Blockage in 2" fill line
A3-1
Secondary failure of 2" fill line
A3-1

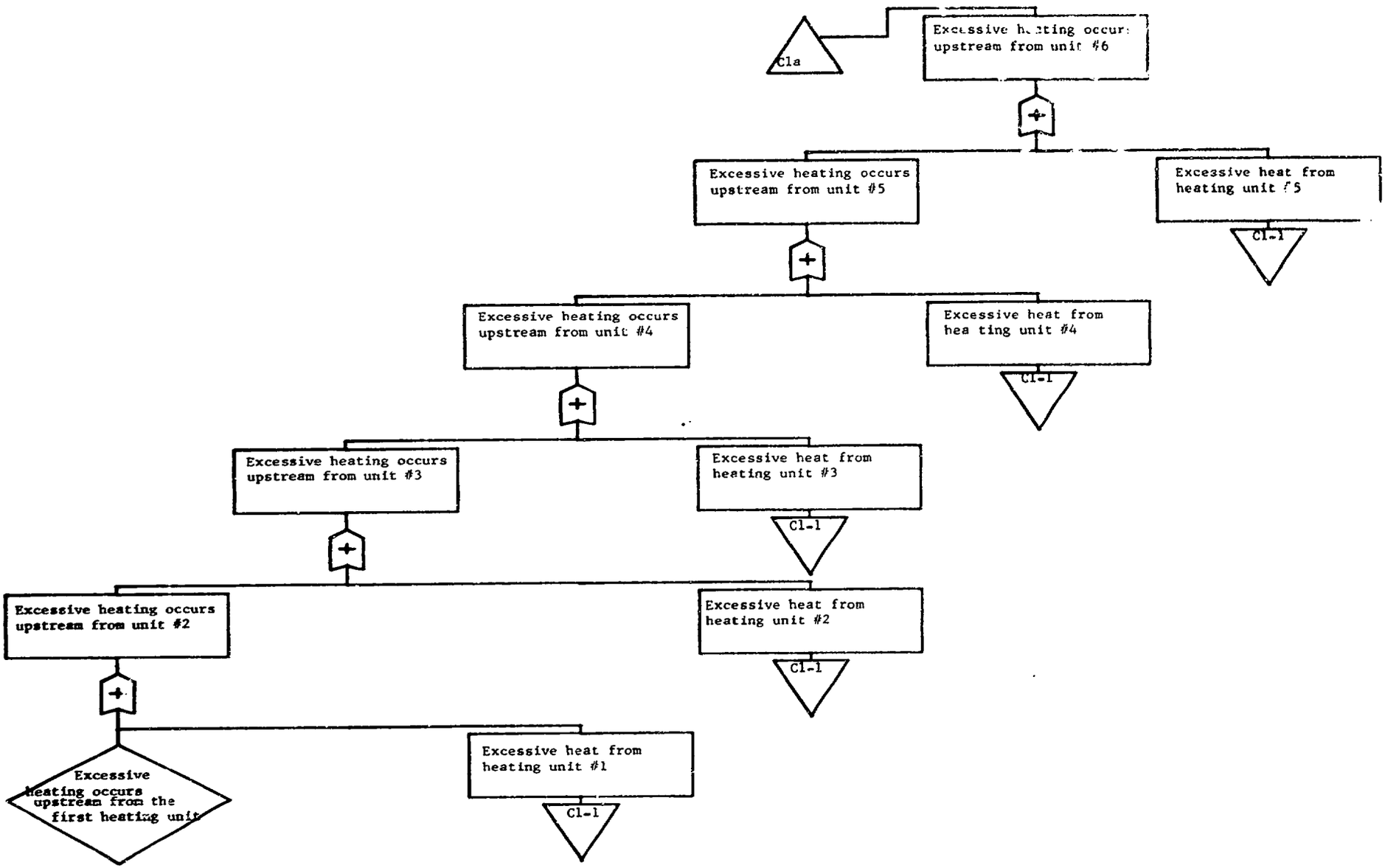

A5d
Product consumed by fire/ explosion in 2" fill line
Explosion in 2" fill line
Transition to explosion
Fire in 2" fill line
A5d-1
Fire in 2" fill line
A5d-1
Sufficient initiation stimulus to cause fire in 2" fill line
Sufficient thermal stimulus to cause cookoff in 2" fill line
Cookoff temperature reached
High product temperature in 2" fill line
Excessive heating from steam tracing and problem not corrected
A1d
Combustible material present

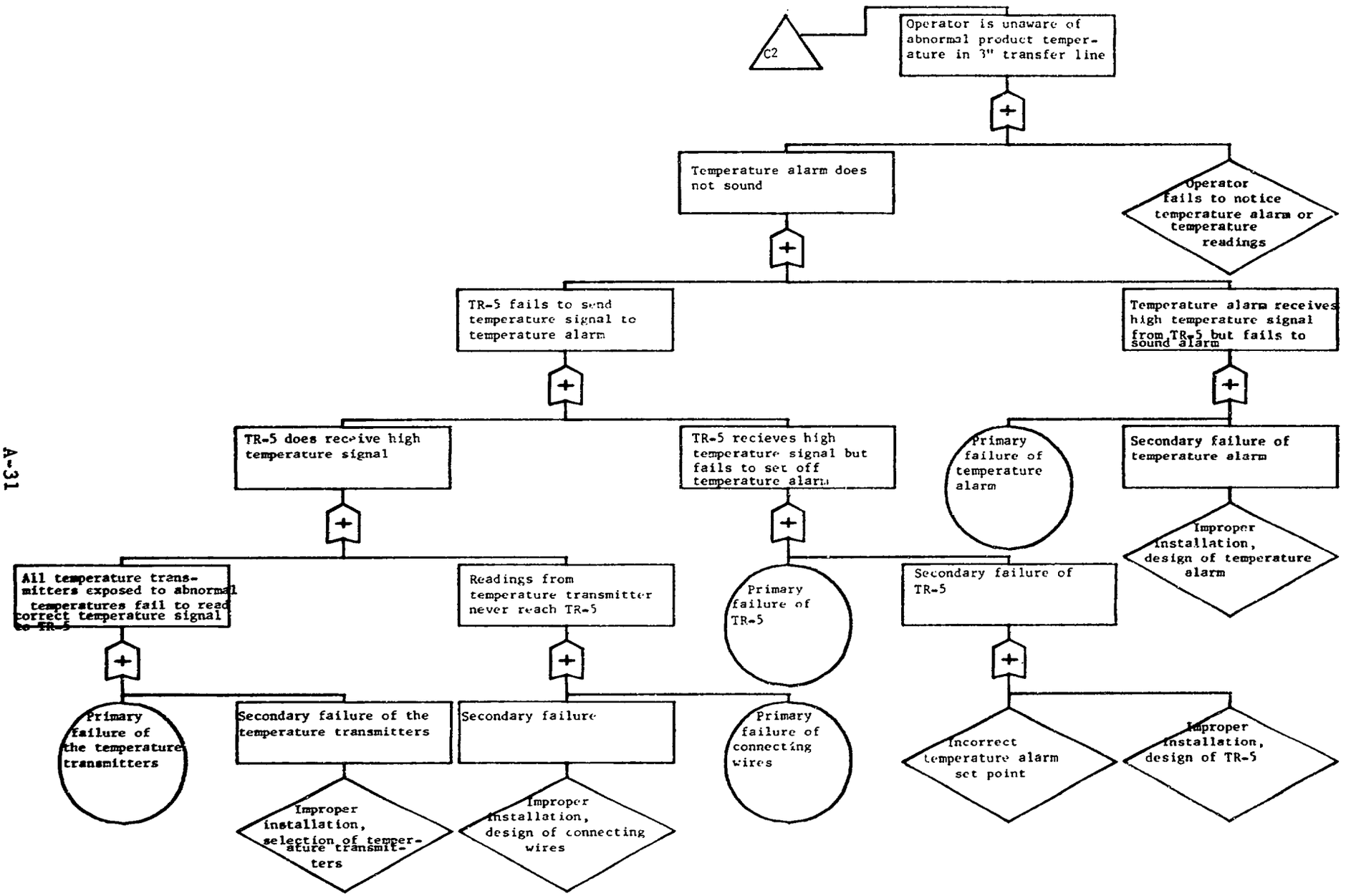

Primary failure of flange(leaks)
Secondary failure of flange
A3-2

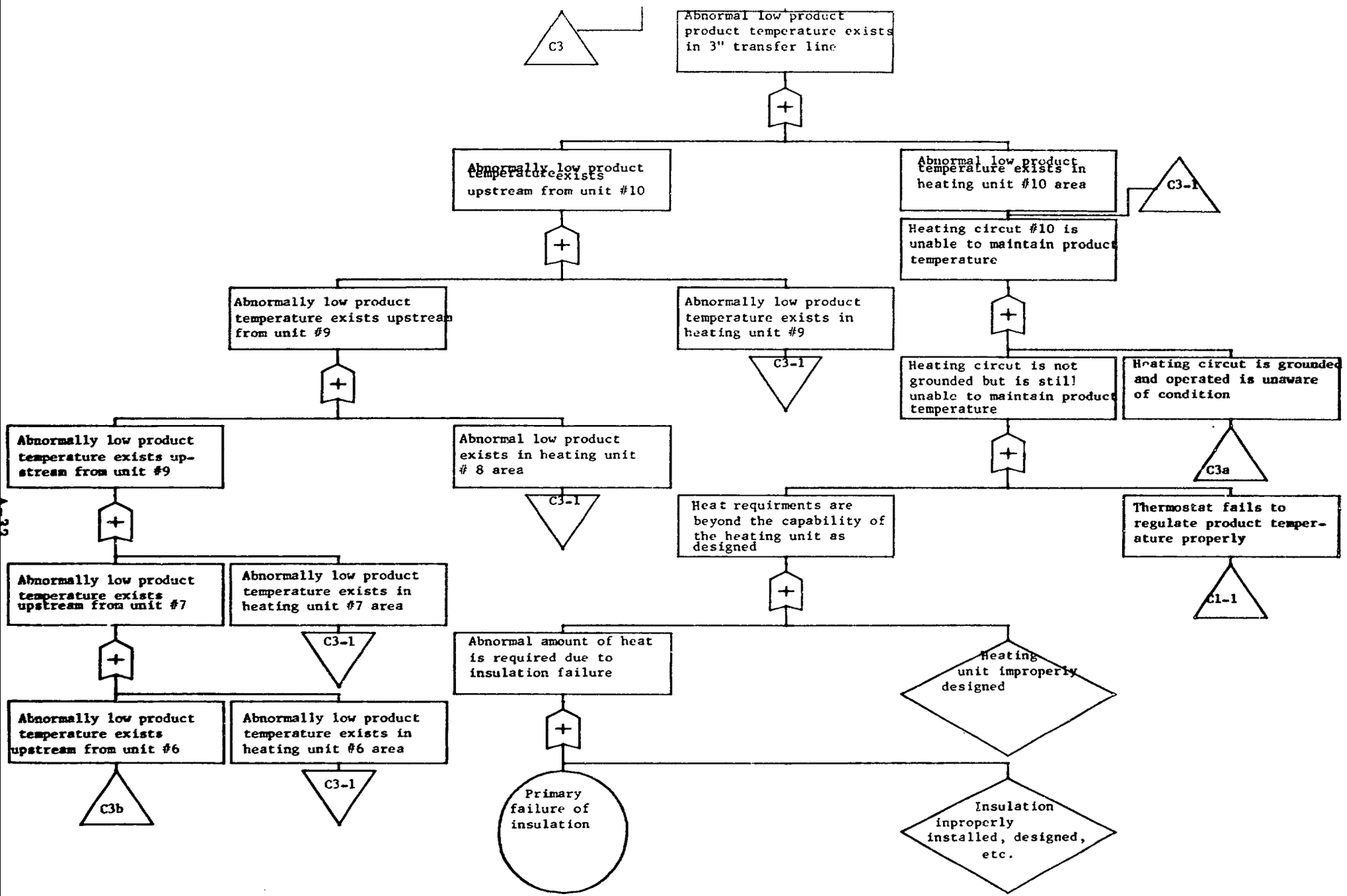

Combustible material present

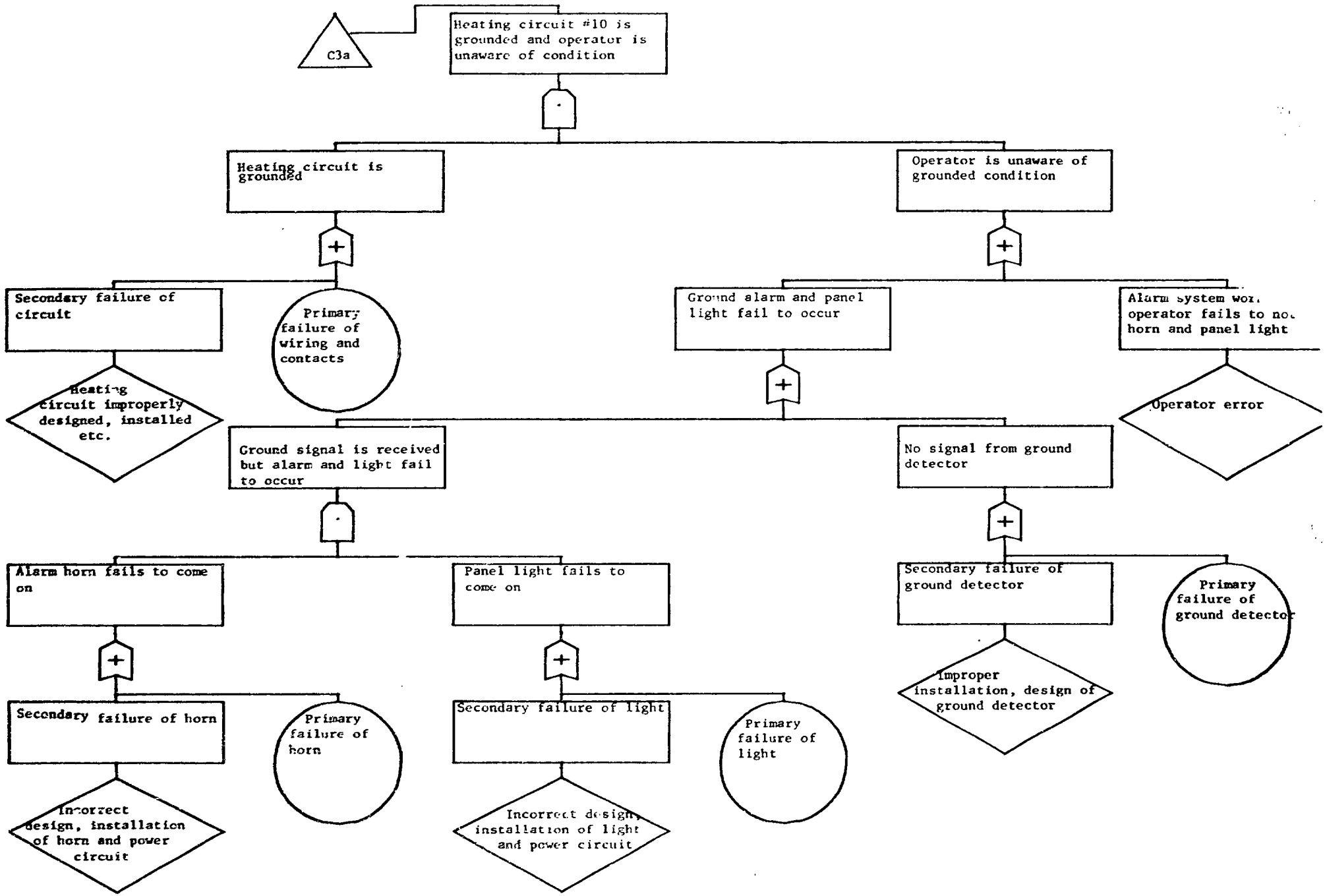

C
3" transfer line fails to pass product
Blockage in 3" transfer line
Secondary failure of 3" transfer line
Primary failure of 3" transfer line
Product is frozen in 3" transfer line
Blockage is possible
Product temperature in 3" transfer pipe drops to freezing point
Abnormally low product temperature exists in 3" transfer line
Abnormal temperature not corrected before freezing point is reached
C3
Abnormal temperature not corrected
Operator is unaware of abnormal product temperature in 3" transfer line
C2
Freezing point will be reached if problem not corrected
Product in 3" transfer line blocked by foreign object
Blockage is possible
Foreign object present in line
Excessive corrosion results in transfer line failure
Sufficient corrosion for failure
Excessive corrosion occurs
C-4
High product temperature exists in 3" transfer line and cause of excessive heating not corrected
Abnormally high product temperature exists in 3" transfer line
C1
3" transfer line improperly designed, selected, etc.
Cause of excessive heating is not connected
Operator is unaware of abnormal product temperature in 3" transfer line
C2

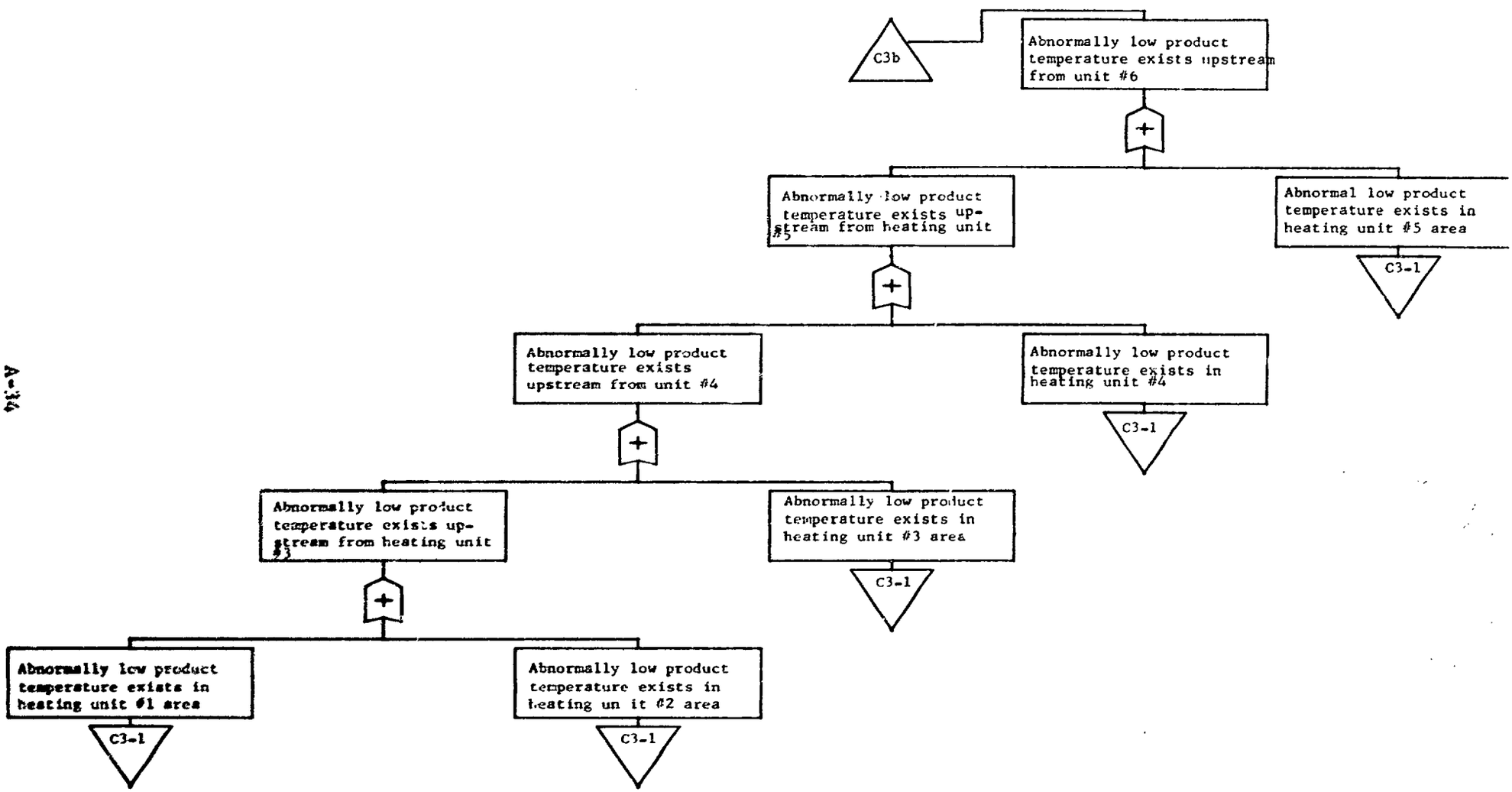

C1
Abnormally high temperature exists in 3" transfer line
Excessive heating occurs upstream from unit #10
Excessive heat from heating unit #10
C1-1
Thermostat fails to regulate product temperature properly
Excessive heating occurs upstream from unit #9
Excessive heat from heating unit #9
C1-1
Improper heating even though proper signal from thermostat is given
Thermostat sends false signal to transformer
Excessive heating occurs upstream from unit #8
Excessive heat from heating unit #8
C1-1
Transfer operates improperly
Secondary failure of thermostat
Primary failure of thermostat
Excessive heat from heating unit #7
Excessive heating occurs upstream from unit #7
C1-1
Primary failure of thermostat
Secondary failure of transformer
Thermostat incorrectly set, installed, etc.
Improper design, installation of Transformer
Excessive heat from heating unit #6
Excessive heating occurs upstream from unit #6
C1-1
C1a

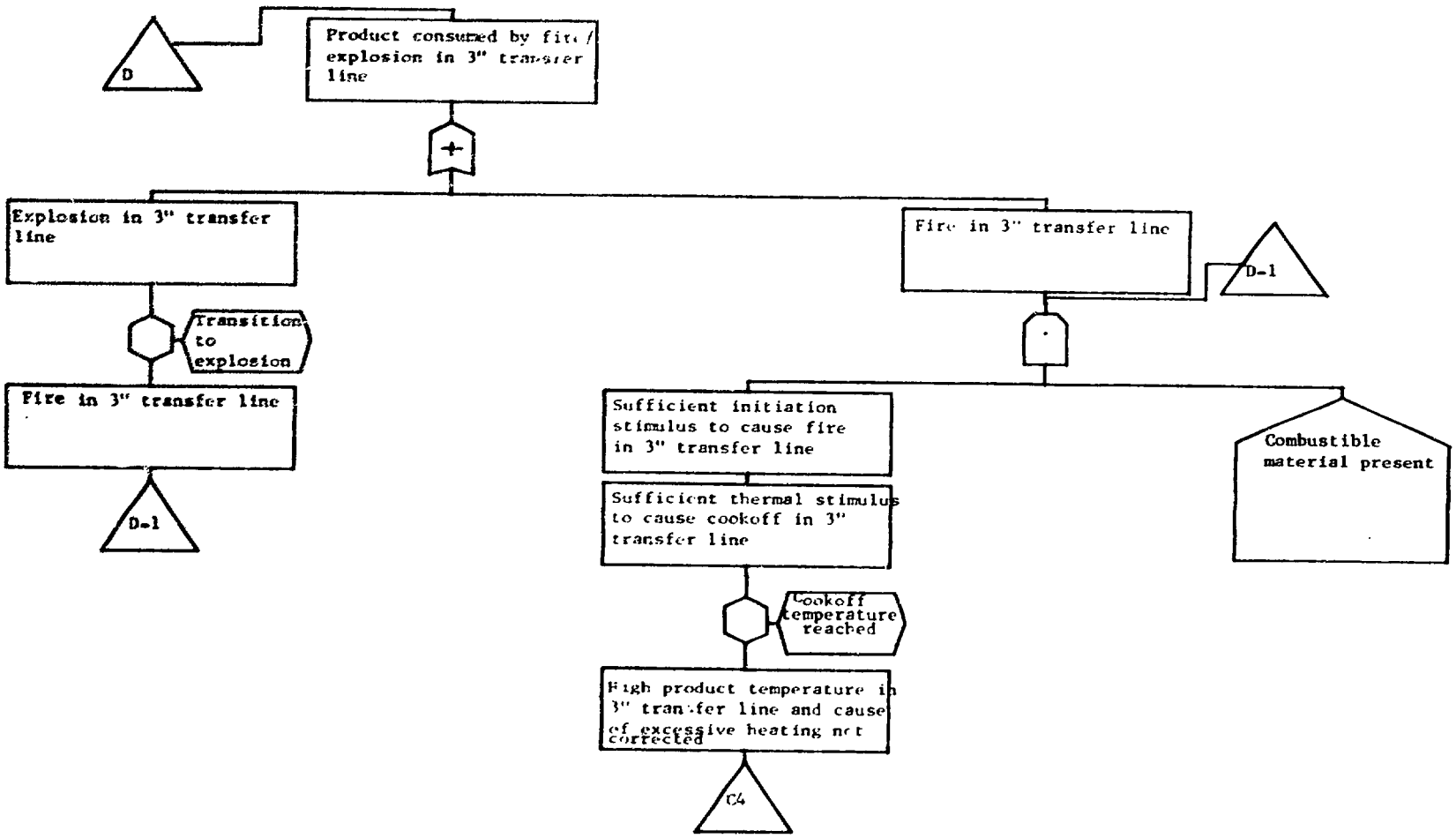

C1a
Excessive heating occurs upstream from unit #6
Excessive heating occurs upstream from unit #5
Excessive heat from heating unit #5
C1-1
Excessive heating occurs upstream from unit #4
Excessive heat from heating unit #4
C1-1
Excessive heating occurs upstream from unit #3
Excessive heat from heating unit #3
C1-1
Excessive heating occurs upstream from unit #2
Excessive heat from heating unit #2
C1-1
Excessive heating occurs upstream from the first heating unit
Excessive heat from heating unit #1
C1-1

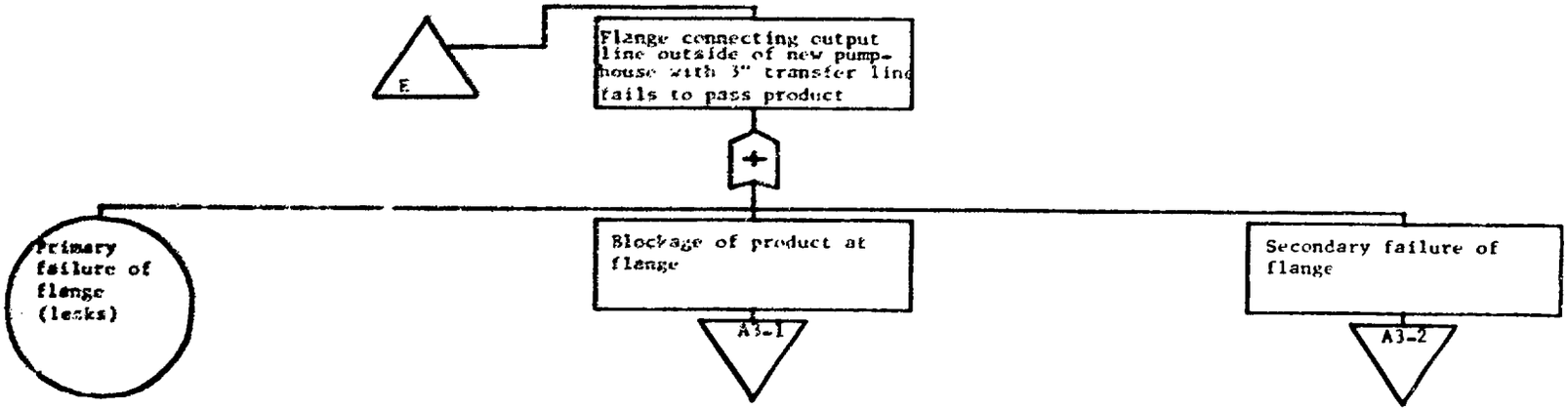

C2
Operator is unaware of abnormal product temperature in 3" transfer line
Temperature alarm does not sound
Operator fails to notice temperature alarm or temperature readings
TR-5 fails to send temperature signal to temperature alarm
Temperature alarm receives high temperature signal from TR-5 but fails to sound alarm
TR-5 does receive high temperature signal
TR-5 recieves high temperature signal but fails to set off temperature alarm
Primary failure of temperature alarm
Secondary failure of temperature alarm
Improper installation, design of temperature alarm
All temperature transmitters exposed to abnormal temperatures fail to read correct temperature signal to TR-5
Readings from temperature transmitter never reach TR-5
Primary failure of TR-5
Secondary failure of TR-5
Primary failure of the temperature transmitters
Secondary failure of the temperature transmitters
Secondary failure
Primary failure of connecting wires
Incorrect temperature alarm set point
Improper installation, design of TR-5
Improper installation, selection of temperature transmitters
Improper installation, design of connecting wires

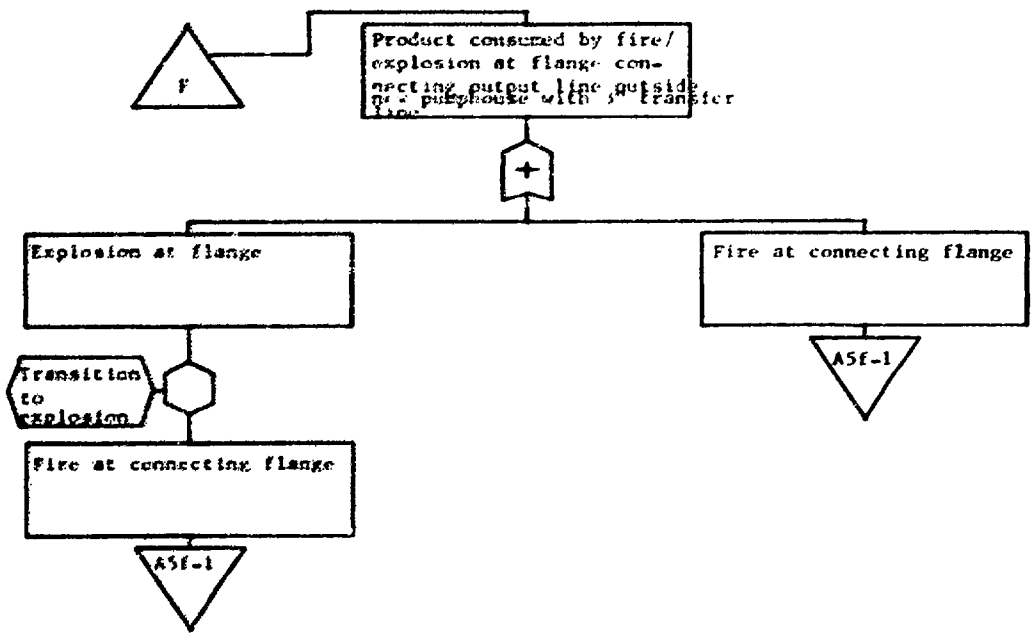

C3
Abnormal low product product temperature exists in 3" transfer line
Abnormally low product temperatdre exists upstream from unit #10
Abnormal low product temperature exists in heating unit #10 area
C3-1
Heating circut #10 is unable to maintain product temperature
Abnormally low product temperature exists upstream from unit #9
Abnormally low product temperature exists in heating unit #9
C3-1
Heating circut is not grounded but is still unable to maintain product temperature
Heating circut is grounded and operated is unaware of condition
C3a
Abnormally low product temperature exists upstream from unit #9
Abnormal low product exists in heating unit # 8 area
C3-1
Heat requirments are beyond the capability of the heating unit as designed
Thermostat fails to regulate product temperature properly
C1-1
Abnormally low product temperature exists upstream from unit #7
Abnormally low product temperature exists in heating unit #7 area
C3-1
Abnormal amount of heat is required due to insulation failure
Heating unit improperly designed
Abnormally low product temperature exists upstream from unit #6
Abnormally low product temperature exists in heating unit #6 area
C3b
C3-1
Primary failure of insulation
Insulation inproperly installed, designed, etc.

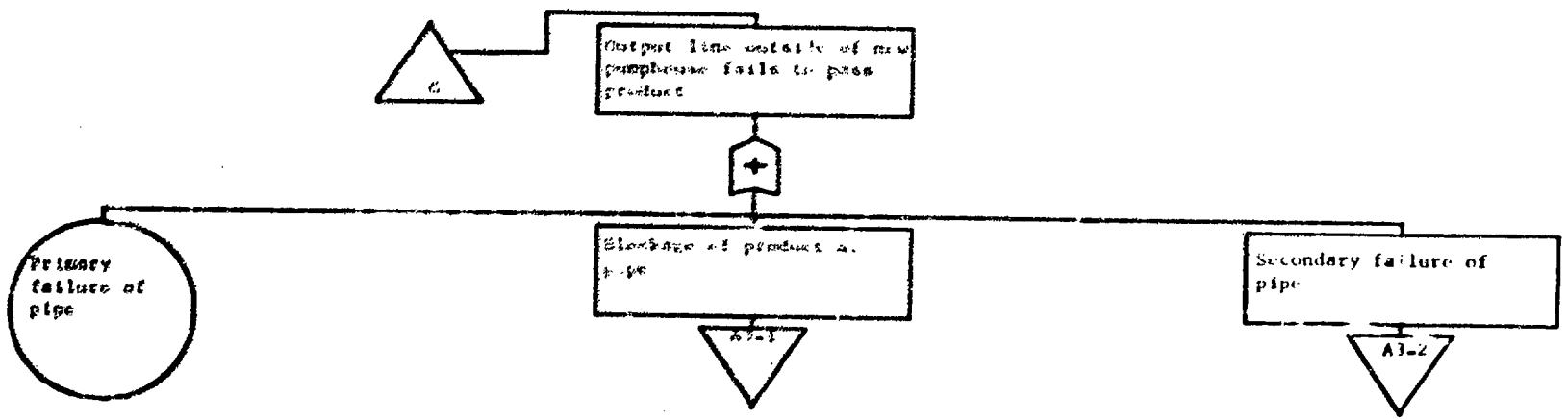

C3a
Heating circuit #10 is grounded and operator is unaware of condition
Heating circuit is grounded
Operator is unaware of grounded condition
Secondary failure of circuit
Primary failure of wiring and contacts
Ground alarm and panel light fail to occur
Alarm system wor
operator fails to no
horn and panel light
Heating circuit improperly designed, installed etc.
Operator error
Ground signal is received but alarm and light fail to occur
No signal from ground detector
Alarm horn fails to come on
Panel light fails to come on
Secondary failure of ground detector
Primary failure of ground detector
Improper installation, design of ground detector
Secondary failure of horn
Primary failure of horn
Secondary failure of light
Primary failure of light
Incorrect design, installation of horn and power circuit
Incorrect design, installation of light and power circuit

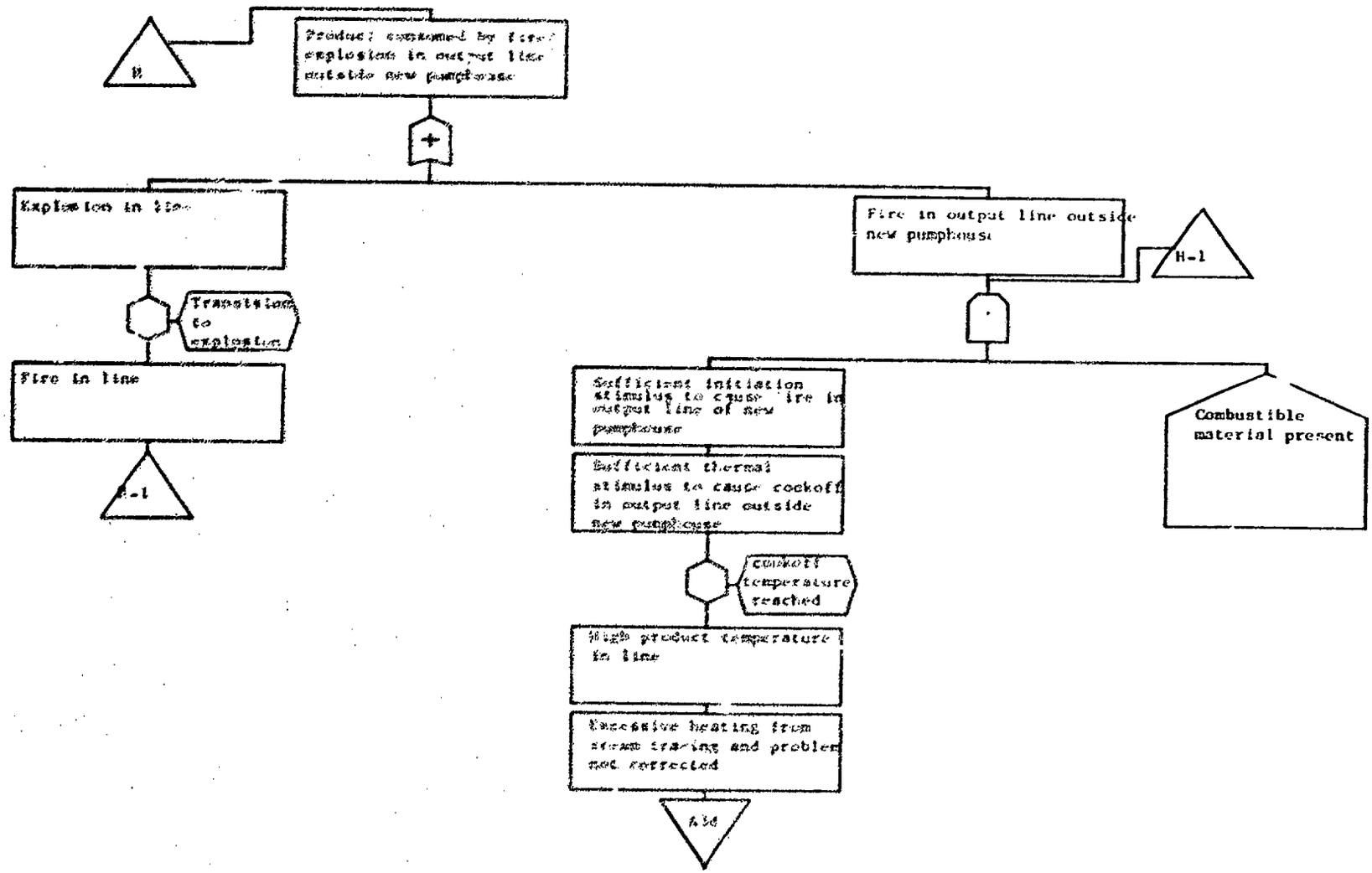

C3b
Abnormally low product temperature exists upstream from unit #6
Abnormally low product temperature exists upstream from heating unit #5
Abnormal low product temperature exists in heating unit #5 area
C3-1
Abnormally low product temperature exists upstream from unit #4
Abnormally low product temperature exists in heating unit #4
C3-1
Abnormally low product temperature exists upstream from heating unit #3
Abnormally low product temperature exists in heating unit #3 area
C3-1
Abnormally low product temperature exists in heating unit #1 area
C3-1
Abnormally low product temperature exists in heating un it #2 area
C3-1

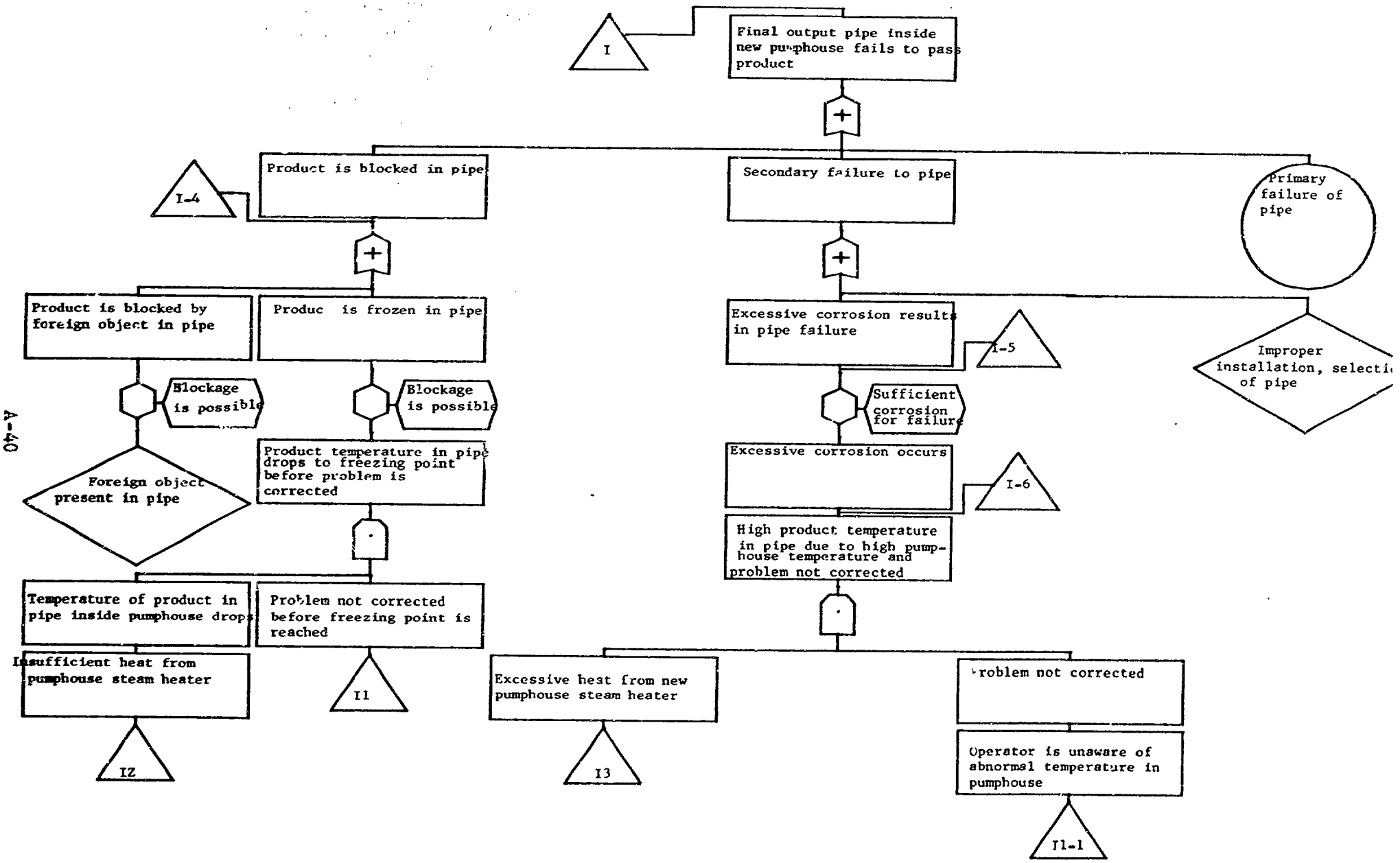

D
Product consumed by fire / explosion in 3" transfer line
Explosion in 3" transfer line
Transition to explosion
Fire in 3" transfer line
D-1
Fire in 3" transfer line
D-1
Sufficient initiation stimulus to cause fire in 3" transfer line
Combustible material present
Sufficient thermal stimulus to cause cookoff in 3" transfer line
Cookoff temperature reached
High product temperature in 3" transfer line and cause of excessive heating not corrected
C4

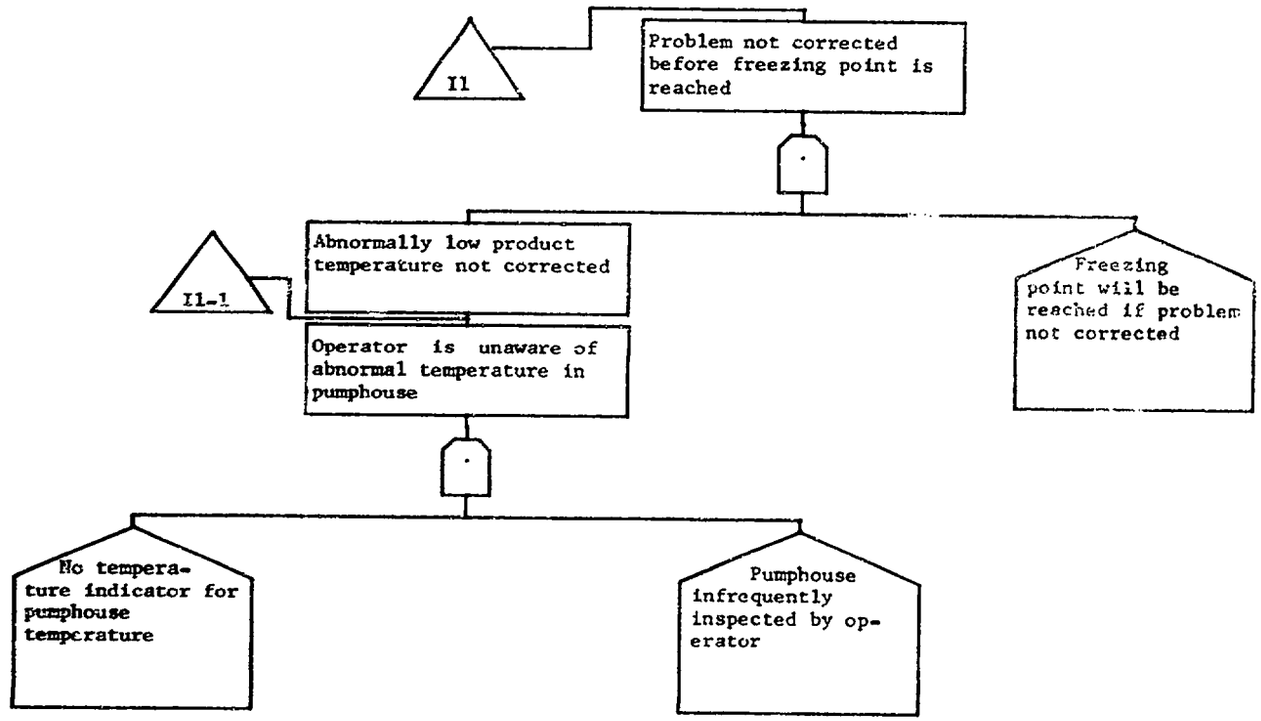

E
Flange connecting output line outside of new pump-house with 3" transfer line fails to pass product
Primary failure of flange (leaks)
Blockage of product at flange
A3-1
Secondary failure of flange
A3-2

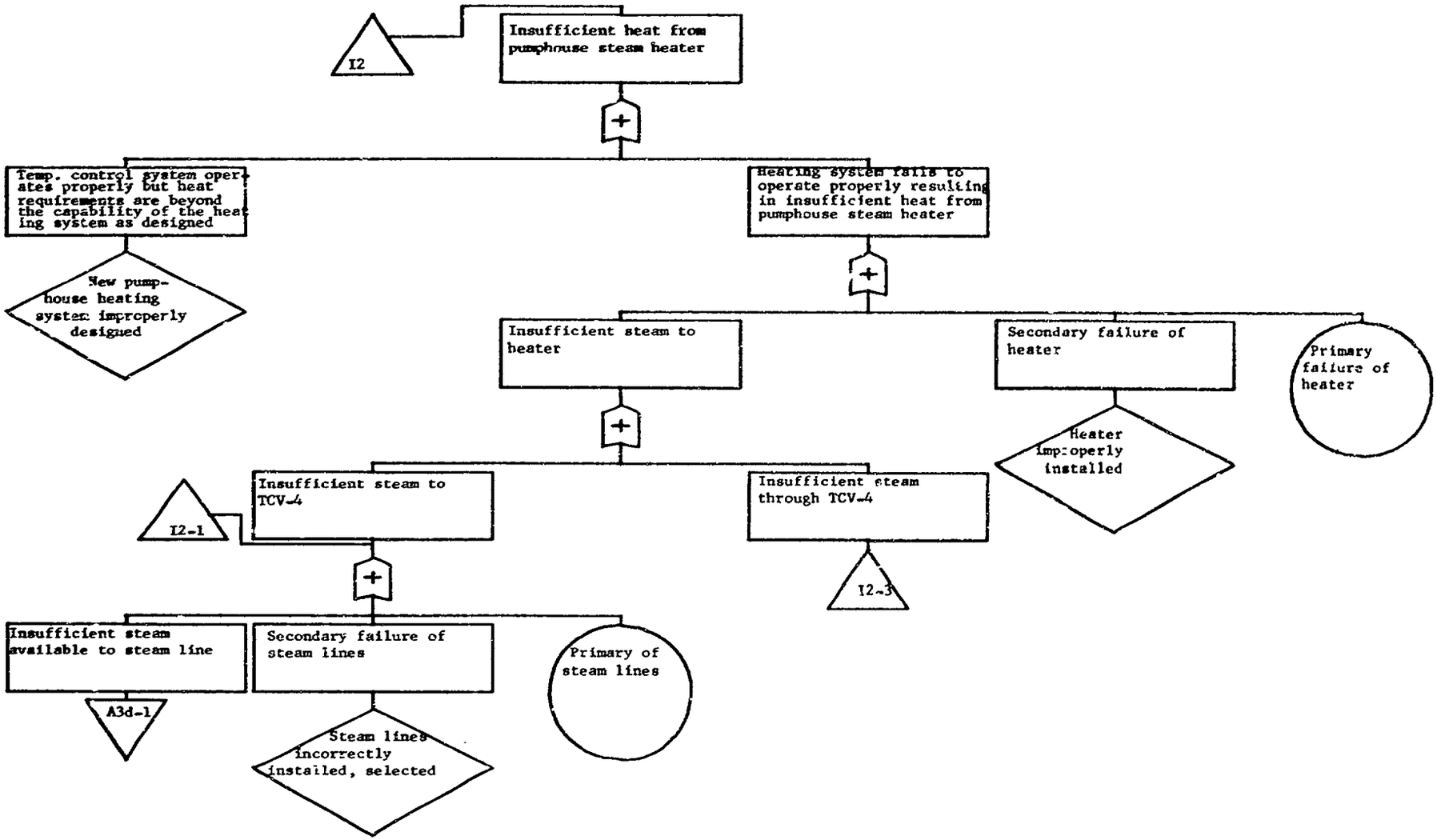

F
Product consumed by fire/ explosion at flange con-
Explosion at flange
Fire at connecting flange
A5f-1
Transition to explosion
Fire at connecting flange
A5f-1

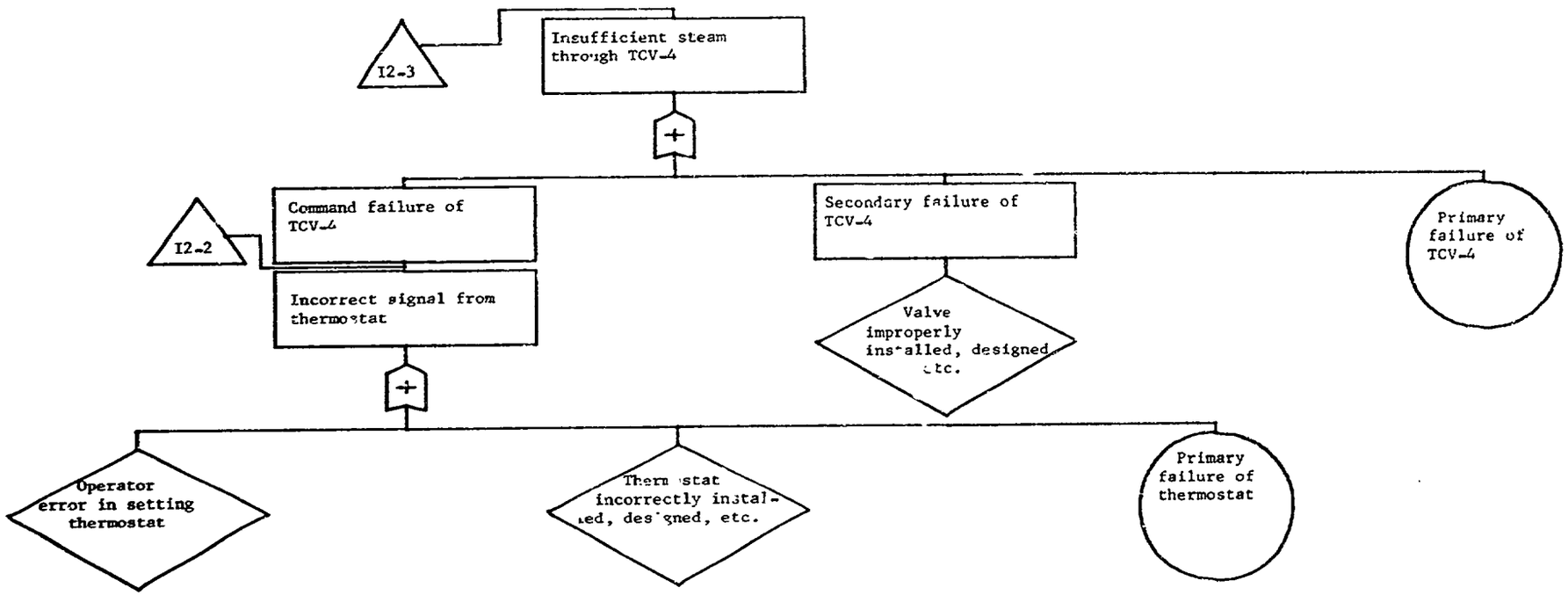

Primary failure of pipe
Secondary failure of pipe
A1-1
A1-2

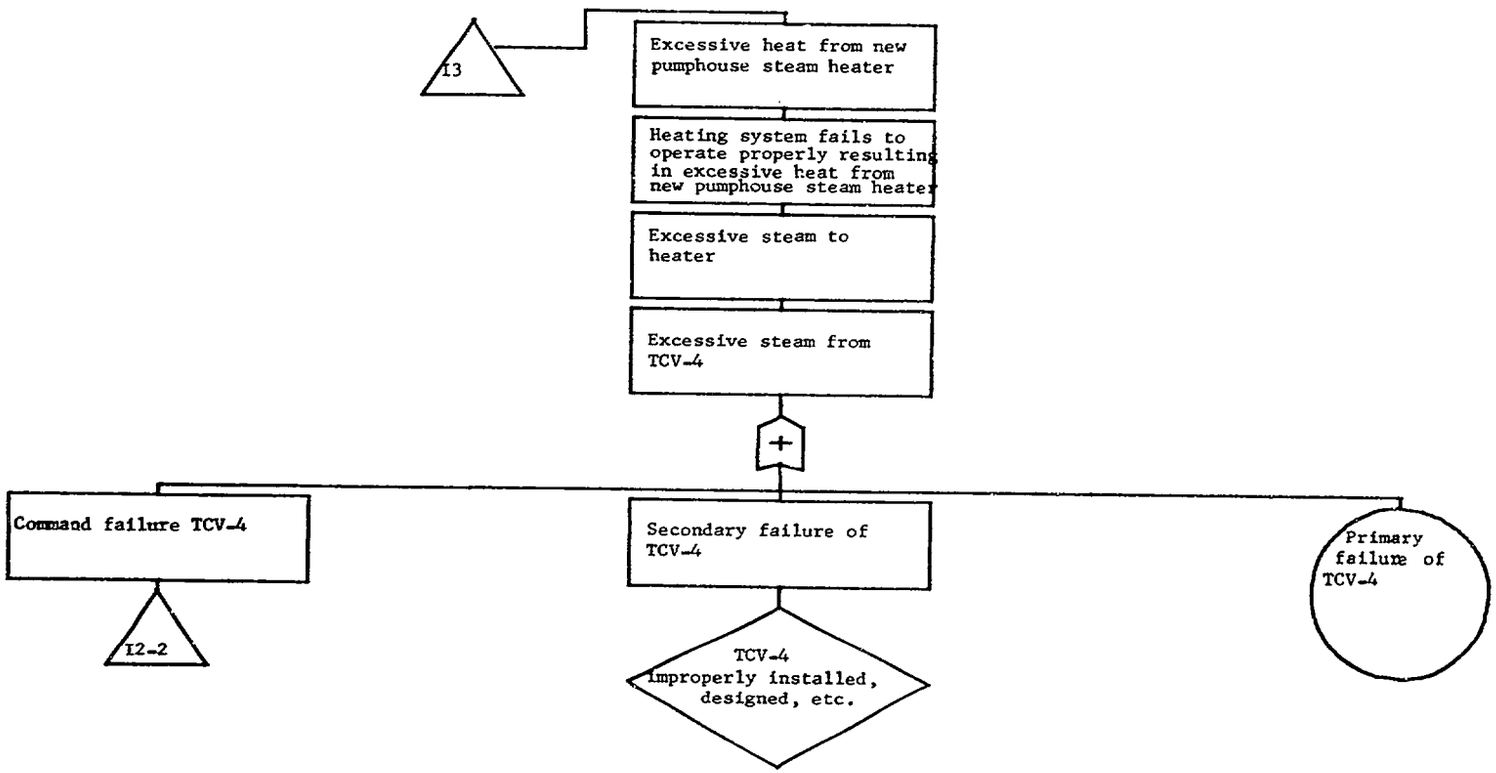

H
Product consumed by fire/explosion in output line outside new pumphouse
Explosion in line
Transition to explosion
Fire in line
H-1
Fire in output line outside new pumphouse
H-1
Sufficient initiation stimulus to cause fire in output line of new pumphouse
Sufficient thermal stimulus to cause cookoff in output line outside new pumphouse
cookoff temperature reached
High product temperature in line
Excessive heating from steam tracing and problem not corrected
A-36
Combustible material present

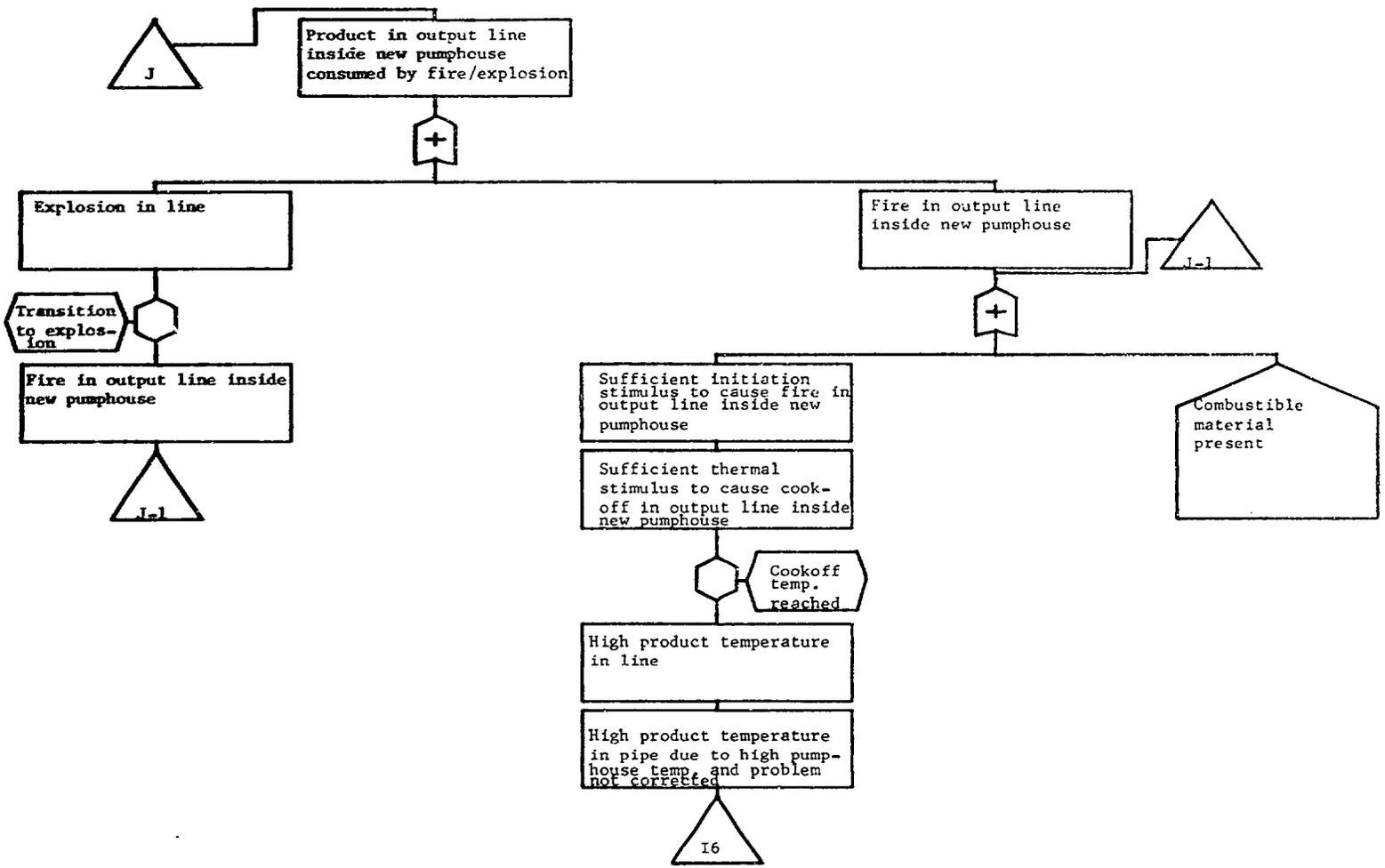

I
Final output pipe inside new pumphouse fails to pass product
I-4
Product is blocked in pipe
Secondary failure to pipe
Primary failure of pipe
Product is blocked by foreign object in pipe
Produc is frozen in pipe
Excessive corrosion results in pipe failure
I-5
Improper installation, selecti of pipe
Blockage is possible
Blockage is possible
Sufficient corrosion for failure
Foreign object present in pipe
Product temperature in pipe drops to freezing point before problem is corrected
Excessive corrosion occurs
I-6
High product temperature in pipe due to high pump-house temperature and problem not corrected
Temperature of product in pipe inside pumphouse drops
Problem not corrected before freezing point is reached
Insufficient heat from pumphouse steam heater
I1
Excessive heat from new pumphouse steam heater
roblem not corrected
IZ
I3
Operator is unaware of abnormal temperature in pumphouse
I1-1

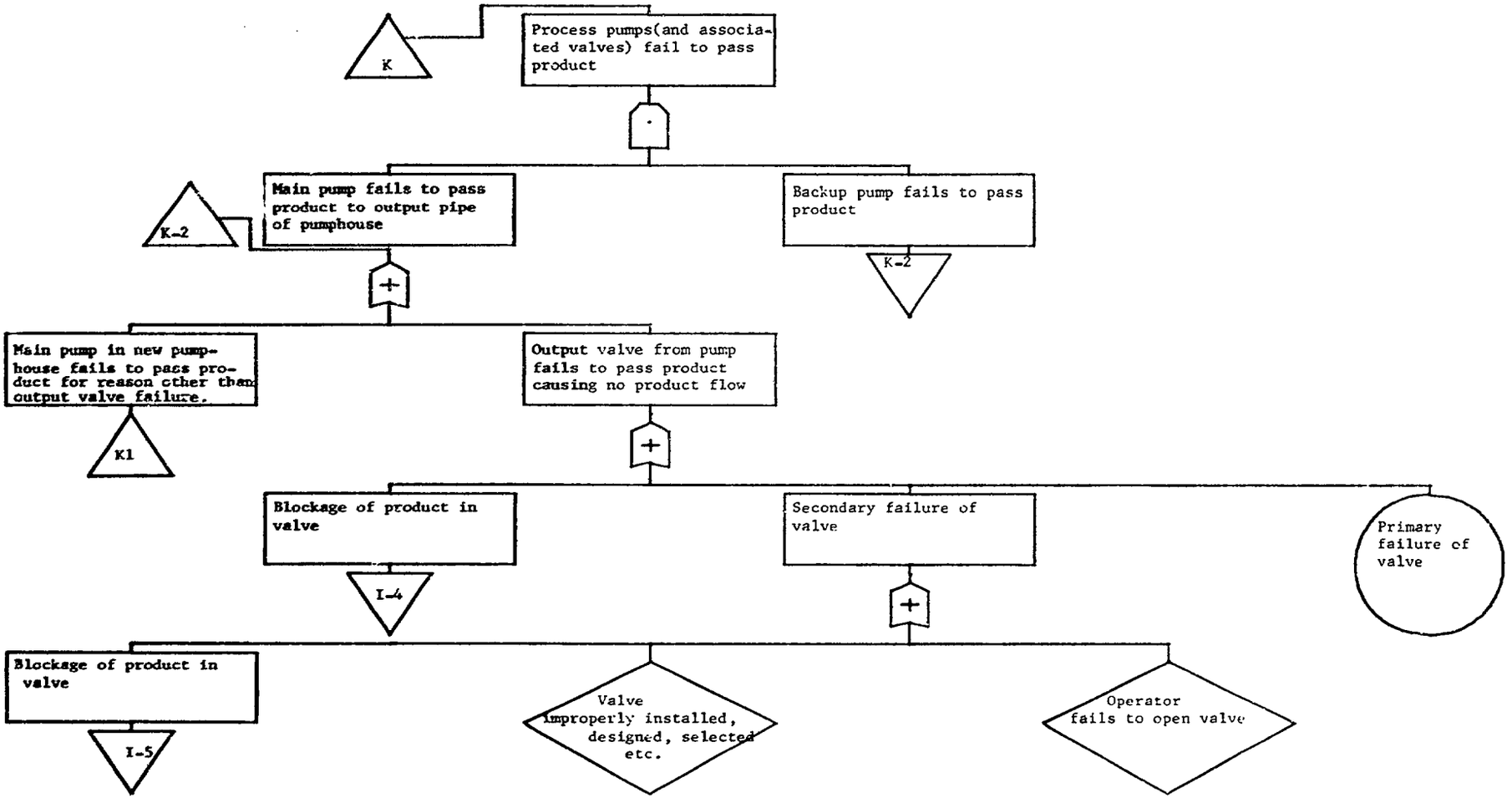

I1
Problem not corrected before freezing point is reached
I1-1
Abnormally low product temperature not corrected
Operator is unaware of abnormal temperature in pumphouse
Freezing point will be reached if problem not corrected
No temperature indicator for pumphouse temperature
Pumphouse infrequently inspected by operator

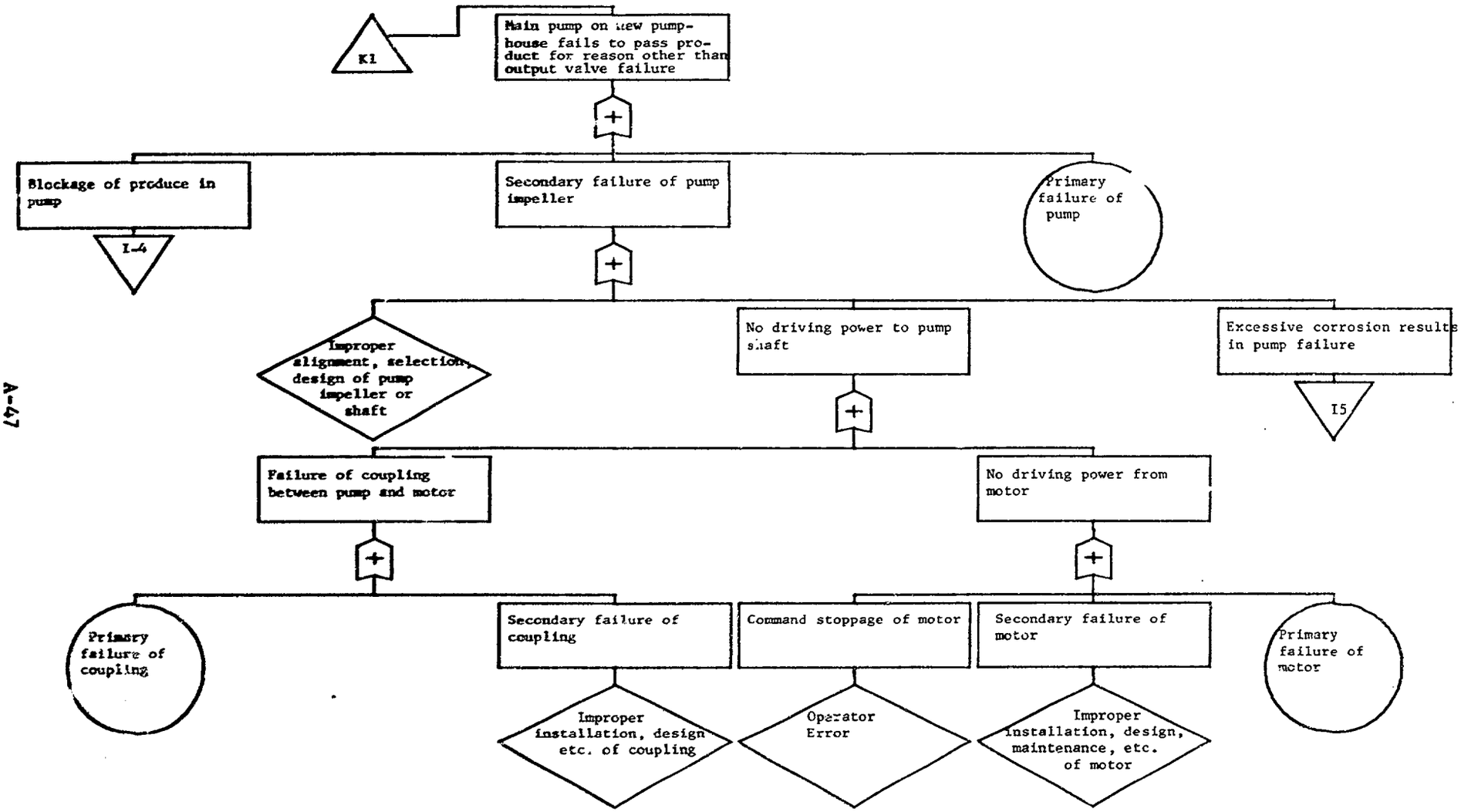

I2
Insufficient heat from pumphouse steam heater
Temp. control system operates properly but heat requirements are beyond the capability of the heating system as designed
New pumphouse heating system improperly designed
Heating system fails to operate properly resulting in insufficient heat from pumphouse steam heater
Insufficient steam to heater
Secondary failure of heater
Primary failure of heater
Heater improperly installed
I2-1
Insufficient steam to TCV-4
Insufficient steam through TCV-4
I2-3
Insufficient steam available to steam line
Secondary failure of steam lines
Primary of steam lines
A3d-1
Steam lines incorrectly installed, selected

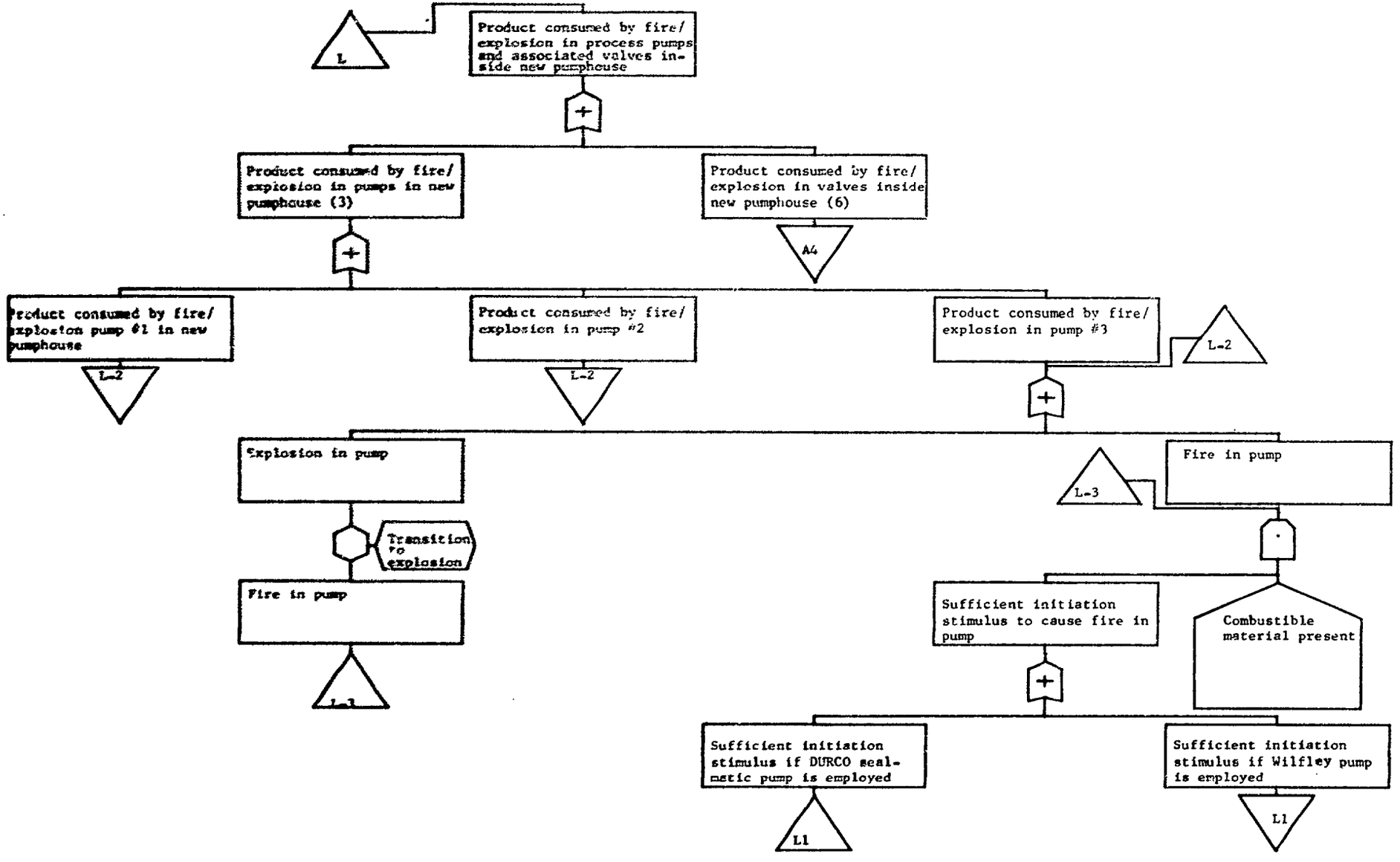

I2-3
Insufficient steam through TCV-4
+
I2-2
Command failure of TCV-4
Incorrect signal from thermostat
+
Operator error in setting thermostat
Thermostat incorrectly installed, designed, etc.
Primary failure of thermostat
Secondary failure of TCV-4
Valve improperly installed, designed, etc.
Primary failure of TCV-4

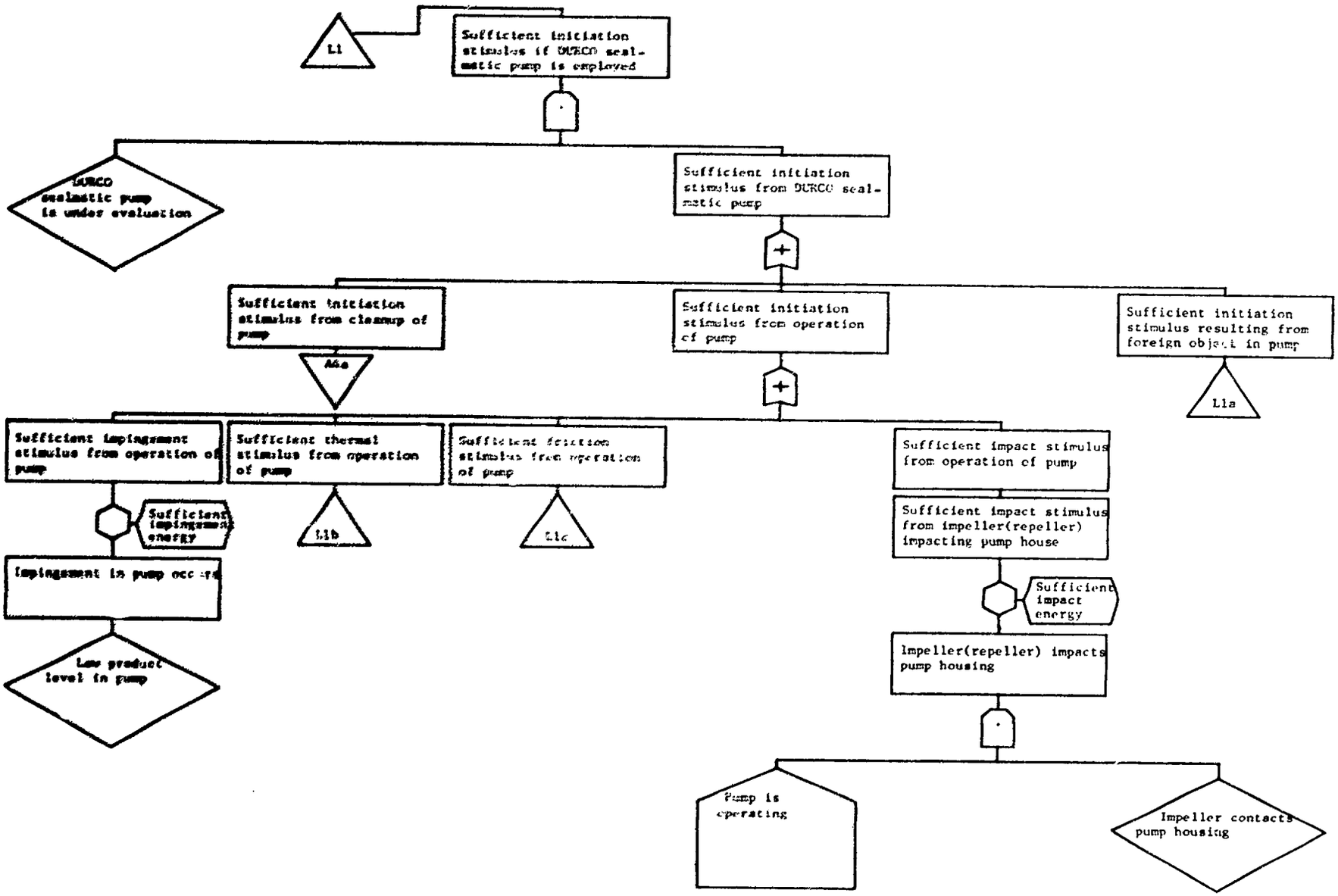

I3
Excessive heat from new pumphouse steam heater
Heating system fails to operate properly resulting in excessive heat from new pumphouse steam heater
Excessive steam to heater
Excessive steam from TCV-4
Command failure TCV-4
I2-2
Secondary failure of TCV-4
TCV-4 improperly installed, designed, etc.
Primary failure of TCV-4

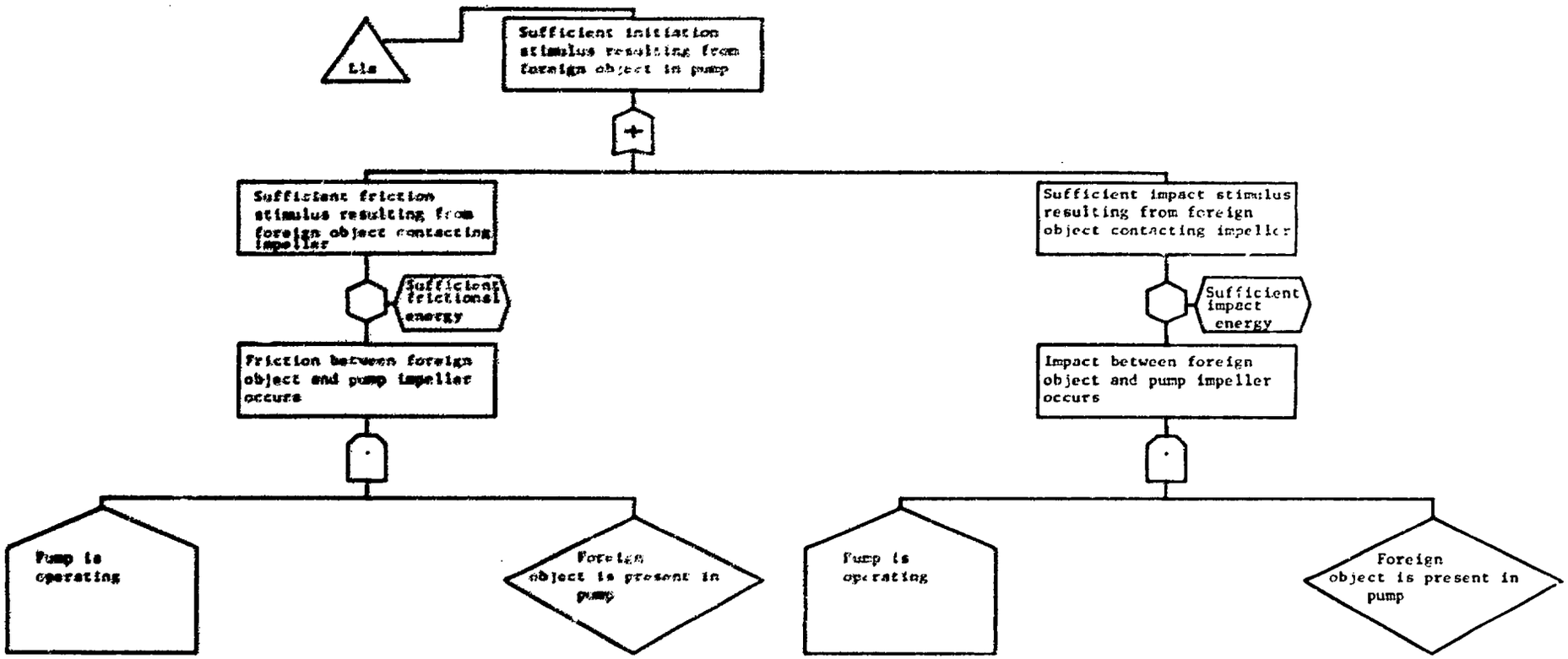

J
Product in output line inside new pumphouse consumed by fire/explosion
Explosion in line
Transition to explosion
Fire in output line inside new pumphouse
J-1
Fire in output line inside new pumphouse
J-1
Sufficient initiation stimulus to cause fire in output line inside new pumphouse
Combustible material present
Sufficient thermal stimulus to cause cook-off in output line inside new pumphouse
Cookoff temp. reached
High product temperature in line
High product temperature in pipe due to high pump-house temp. and problem not corrected
I6

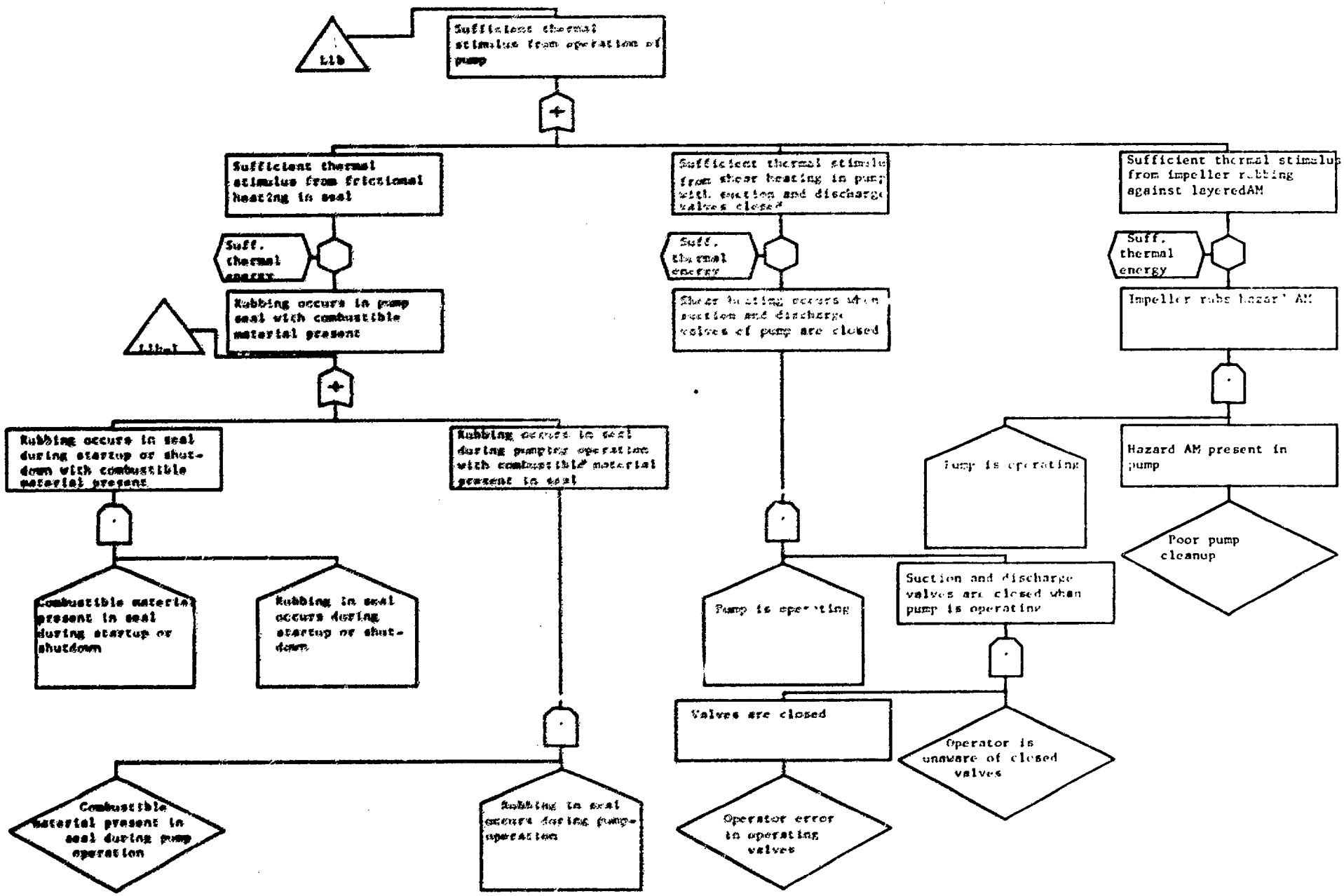

K
Process pumps(and associated valves) fail to pass product
K-2
Main pump fails to pass product to output pipe of pumphouse
Backup pump fails to pass product
K-2
Main pump in new pumphouse fails to pass product for reason other than output valve failure.
K1
Output valve from pump fails to pass product causing no product flow
Blockage of product in valve
I-4
Secondary failure of valve
Primary failure of valve
Blockage of product in valve
I-5
Valve improperly installed, designed, selected etc.
Operator fails to open valve

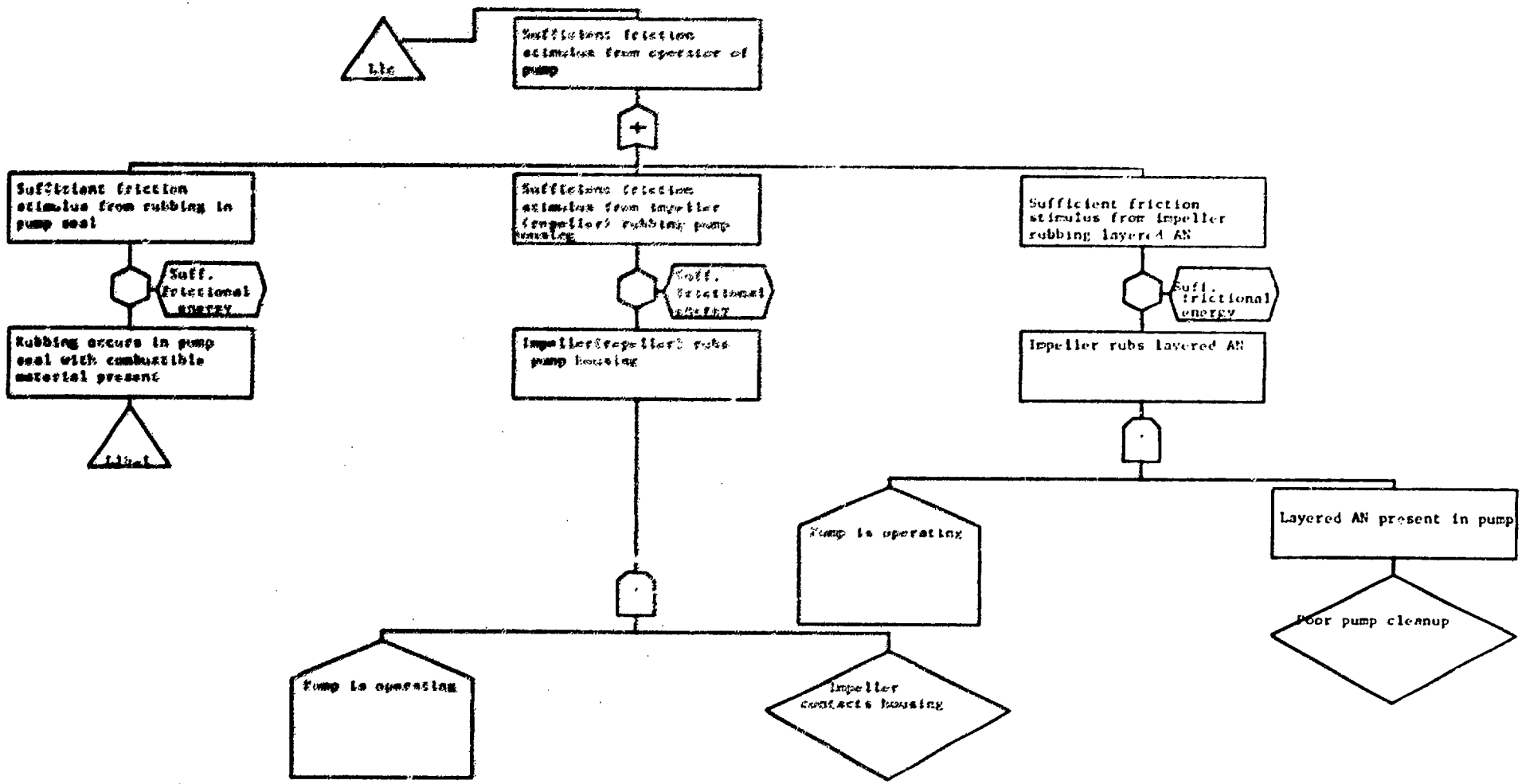

K1
Main pump on new pump-house fails to pass product for reason other than output valve failure
Blockage of produce in pump
I-4
Secondary failure of pump impeller
Primary failure of pump
Improper alignment, selection, design of pump impeller or shaft
No driving power to pump shaft
Excessive corrosion results in pump failure
I5
Failure of coupling between pump and motor
No driving power from motor
Primary failure of coupling
Secondary failure of coupling
Command stoppage of motor
Secondary failure of motor
Primary failure of motor
Improper installation, design etc. of coupling
Operator Error
Improper installation, design, maintenance, etc. of motor

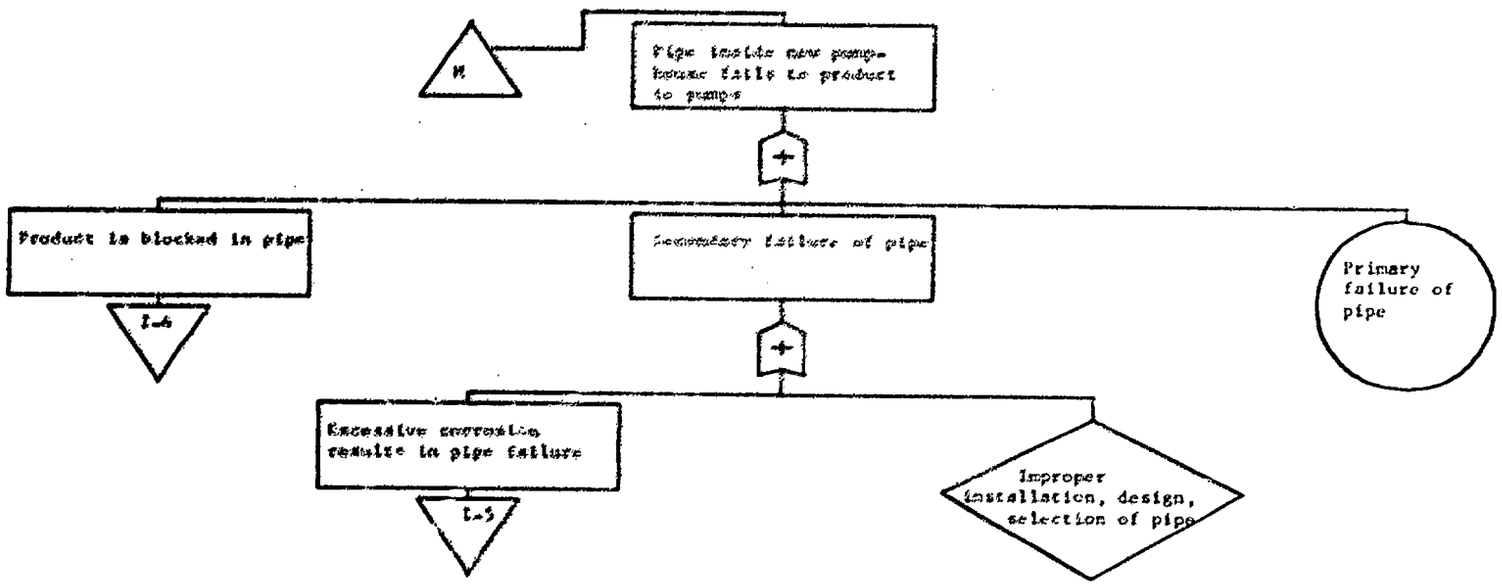

L
Product consumed by fire/ explosion in process pumps and associated valves inside new pumphouse
Product consumed by fire/ explosion in pumps in new pumphouse (3)
Product consumed by fire/ explosion in valves inside new pumphouse (6)
A4
Product consumed by fire/ explosion pump #1 in new pumphouse
L-2
Product consumed by fire/ explosion in pump #2
L-2
Product consumed by fire/ explosion in pump #3
L-2
Explosion in pump
Transition to explosion
Fire in pump
L-3
L-3
Fire in pump
Sufficient initiation stimulus to cause fire in pump
Combustible material present
Sufficient initiation stimulus if DURCO sealmatic pump is employed
L1
Sufficient initiation stimulus if Wilfley pump is employed
L1

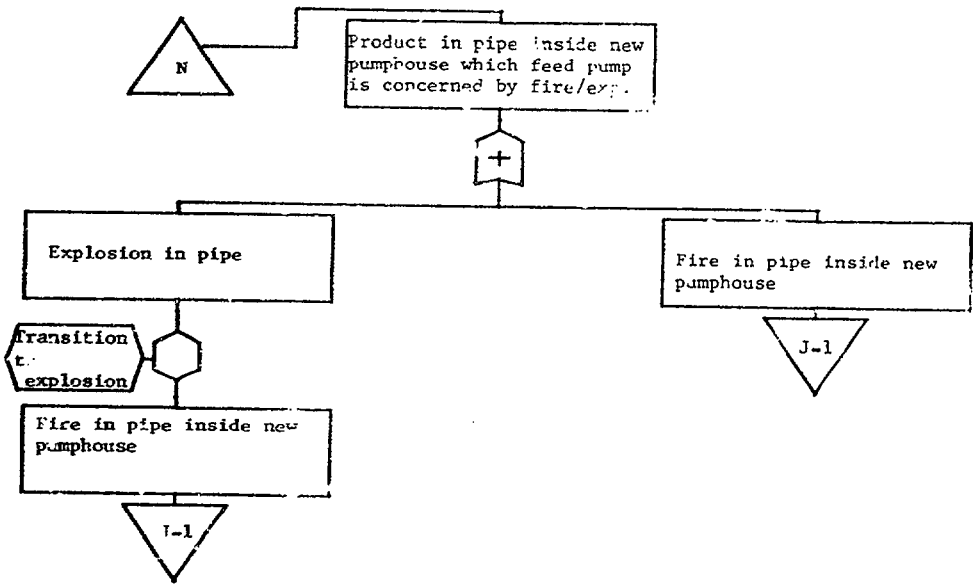

L1
Sufficient initiation stimulus if DURCO sealmatic pump is employed
DURCO sealmatic pump is under evaluation
Sufficient initiation stimulus from DURCO sealmatic pump
Sufficient initiation stimulus from cleanup of pump
A6a
Sufficient initiation stimulus from operation of pump
Sufficient initiation stimulus resulting from foreign object in pump
L1a
Sufficient impingement stimulus from operation of pump
Sufficient thermal stimulus from operation of pump
Sufficient friction stimulus from operation of pump
Sufficient impact stimulus from operation of pump
Sufficient impingement energy
L1b
L1c
Sufficient impact stimulus from impeller(repeller) impacting pump house
Impingement in pump occurs
Sufficient impact energy
Low product level in pump
Impeller(repeller) impacts pump housing
Pump is operating
Impeller contacts pump housing

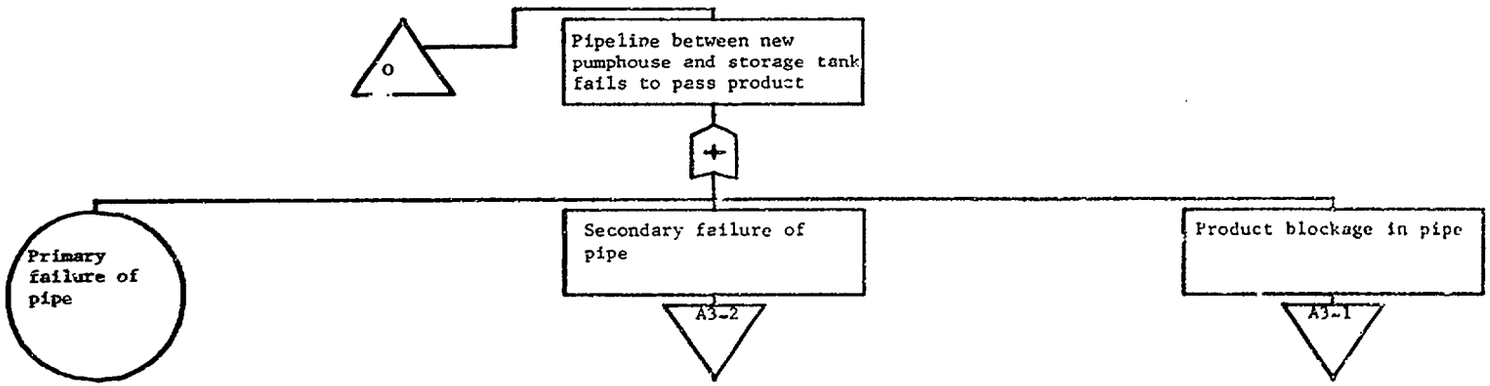

L1a
Sufficient initiation stimulus resulting from foreign object in pump
+
Sufficient friction stimulus resulting from foreign object contacting impeller
Sufficient frictional energy
Friction between foreign object and pump impeller occurs
Pump is operating
Foreign object is present in pump
Sufficient impact stimulus resulting from foreign object contacting impeller
Sufficient impact energy
Impact between foreign object and pump impeller occurs
Pump is operating
Foreign object is present in pump

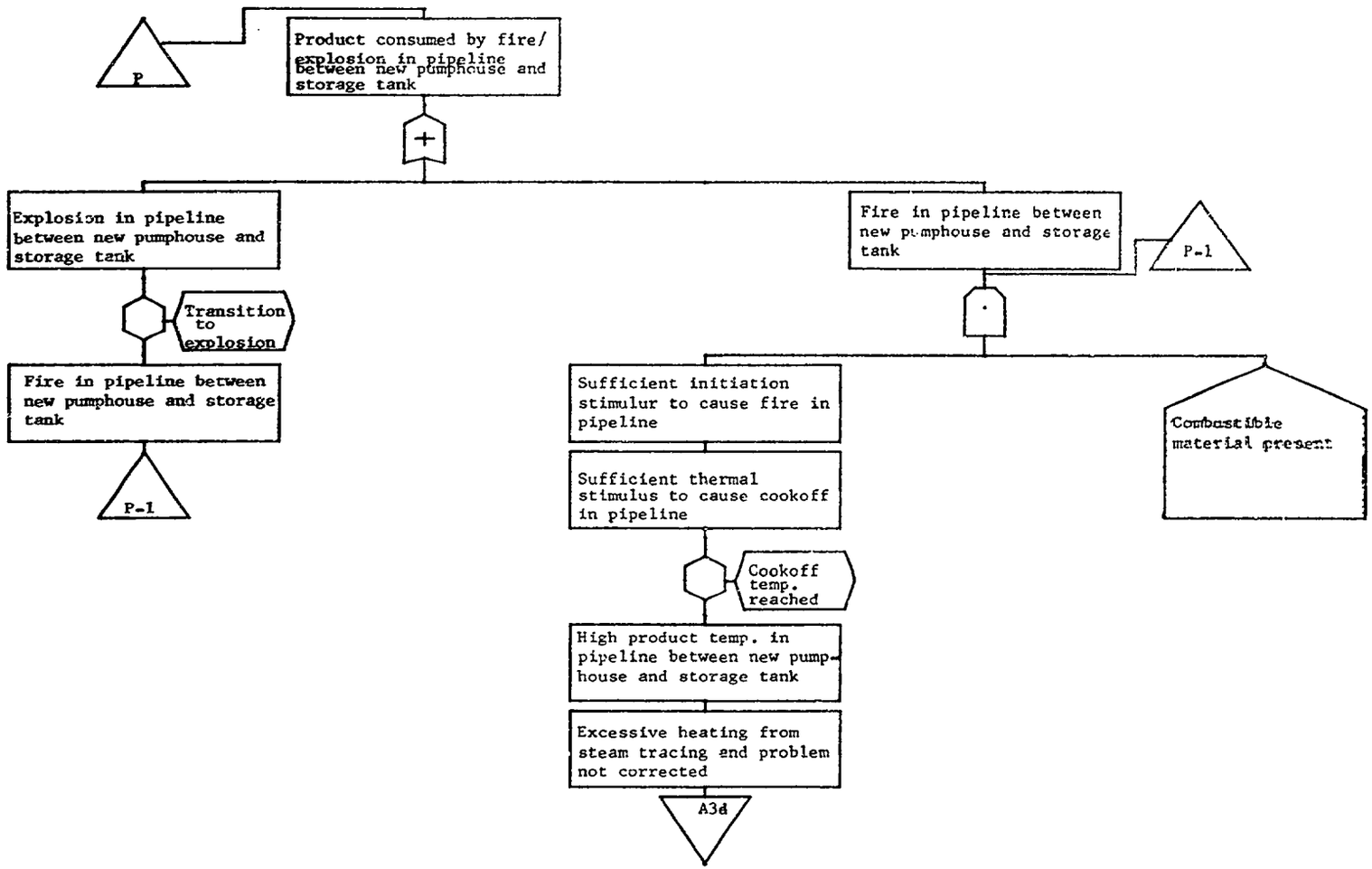

Lib
Sufficient thermal stimulus from operation of pump
Sufficient thermal stimulus from frictional heating in seal
Sufficient thermal stimulus from shear heating in pump with suction and discharge valves closed
Sufficient thermal stimulus from impeller rubbing against layeredAM
Suff. thermal energy
Suff. thermal energy
Suff. thermal energy
Rubbing occurs in pump seal with combustible material present
Lib
Shear heating occurs when suction and discharge valves of pump are closed
Impeller rubs hazard AM
Rubbing occurs in seal during startup or shutdown with combustible material present
Rubbing occurs in seal during pumping operation with combustible material present in seal
Pump is operating
Hazard AM present in pump
Poor pump cleanup
Combustible material present in seal during startup or shutdown
Rubbing in seal occurs during startup or shutdown
Pump is operating
Suction and discharge valves are closed when pump is operating
Valves are closed
Operator is unaware of closed valves
Operator error in operating valves
Combustible material present in seal during pump operation
Rubbing in seal occurs during pump operation

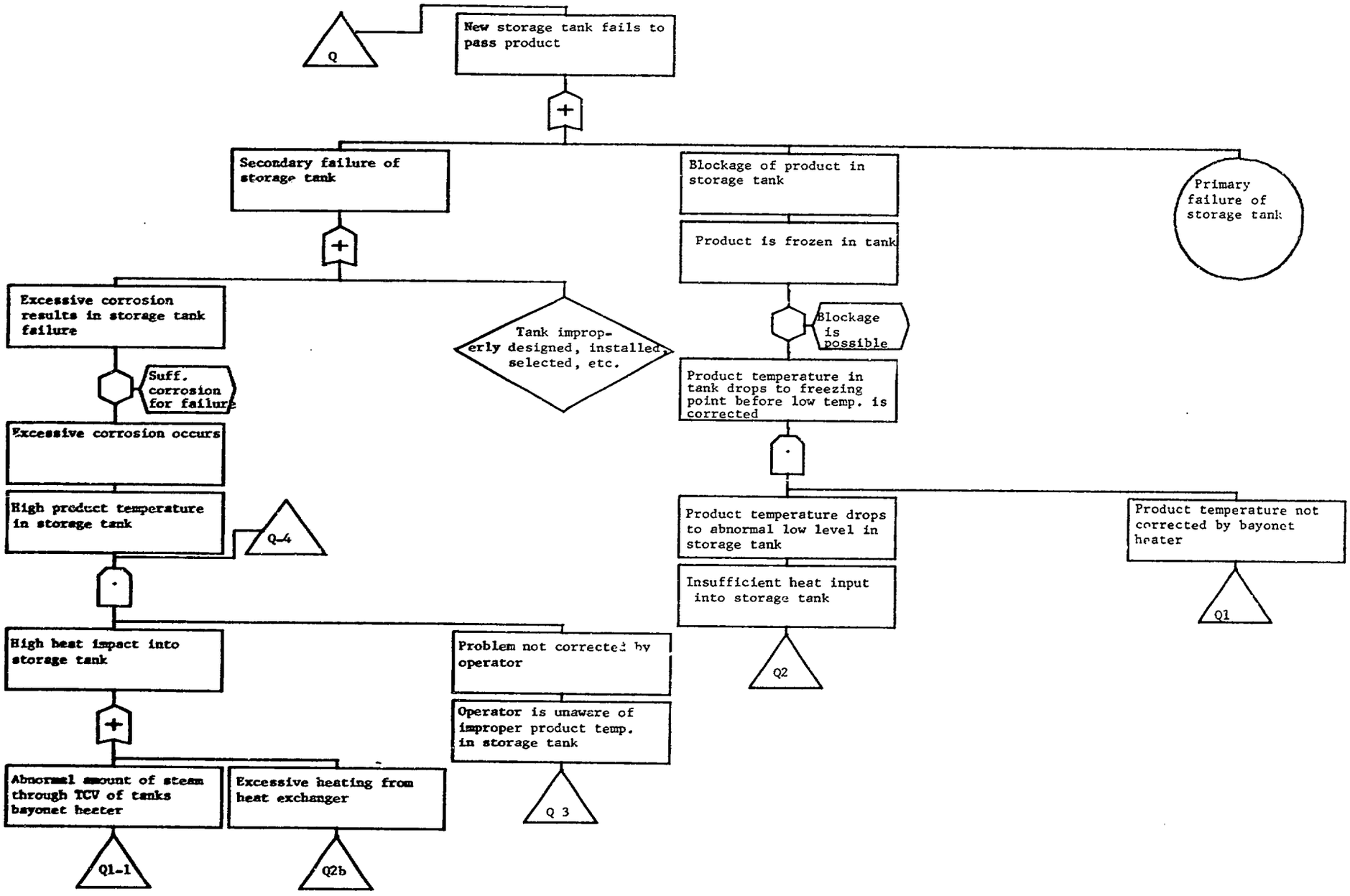

Sufficient friction stimulus from operation of pump
Sufficient friction stimulus from rubbing in pump seal
Suff. frictional energy
Rubbing occurs in pump seal with combustible material present
Sufficient friction stimulus from impeller (impeller) rubbing pump housing
Suff. frictional energy
Impeller/impeller rubs pump housing
Sufficient friction stimulus from impeller rubbing layered AN
Suff. frictional energy
Impeller rubs layered AN
Pump is operating
Layered AN present in pump
Poor pump cleanup
Pump is operating
Impeller contacts housing

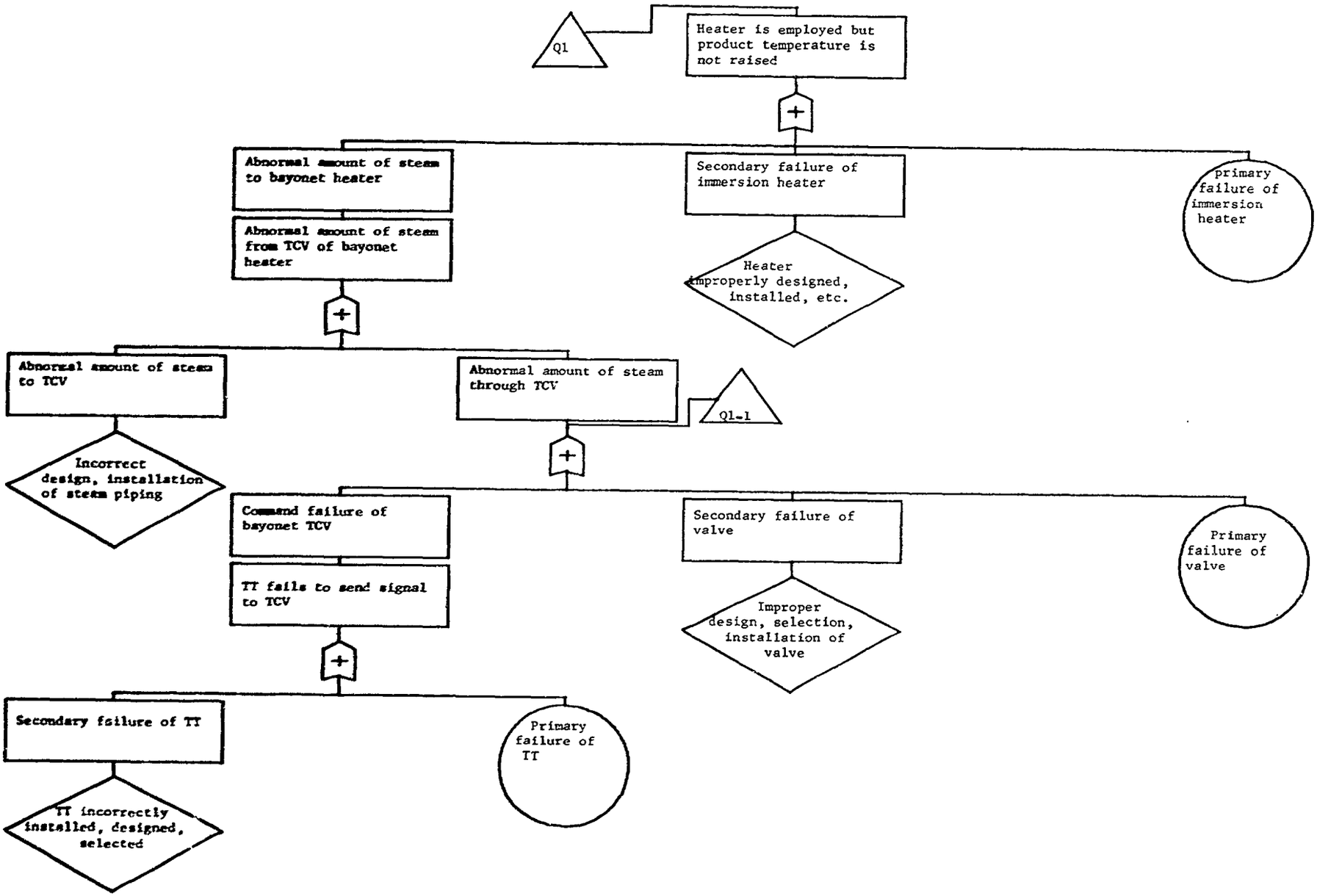

M
Pipe inside new pump-house fails to product to pump
Product is blocked in pipe
Secondary failure of pipe
Primary failure of pipe
Excessive corrosion results in pipe failure
Improper installation, design, selection of pipe

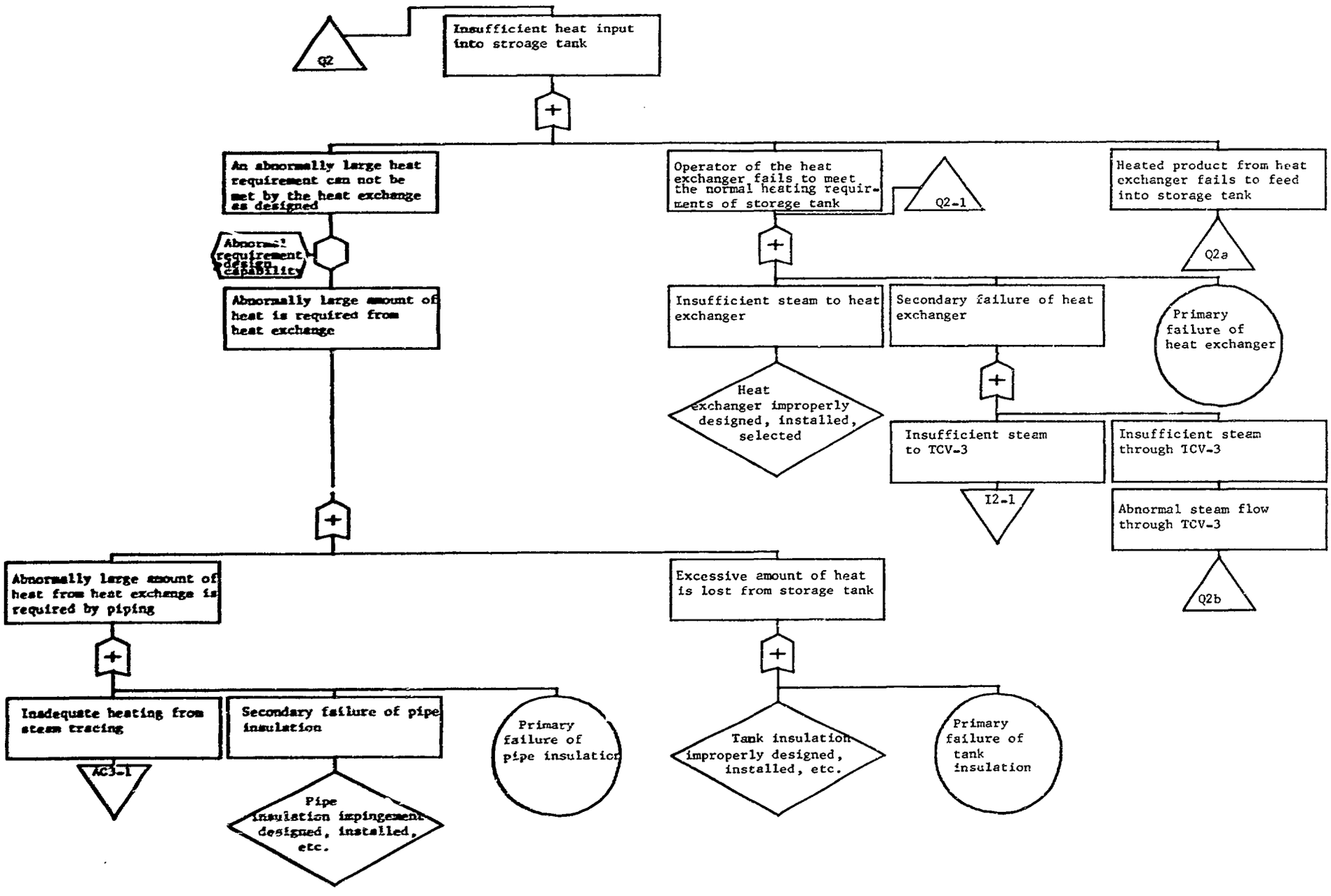

N
Product in pipe inside new pumphouse which feed pump is concerned by fire/exp.
+
Explosion in pipe
Fire in pipe inside new pumphouse
J-1
Transition t.. explosion
Fire in pipe inside new pumphouse
J-1

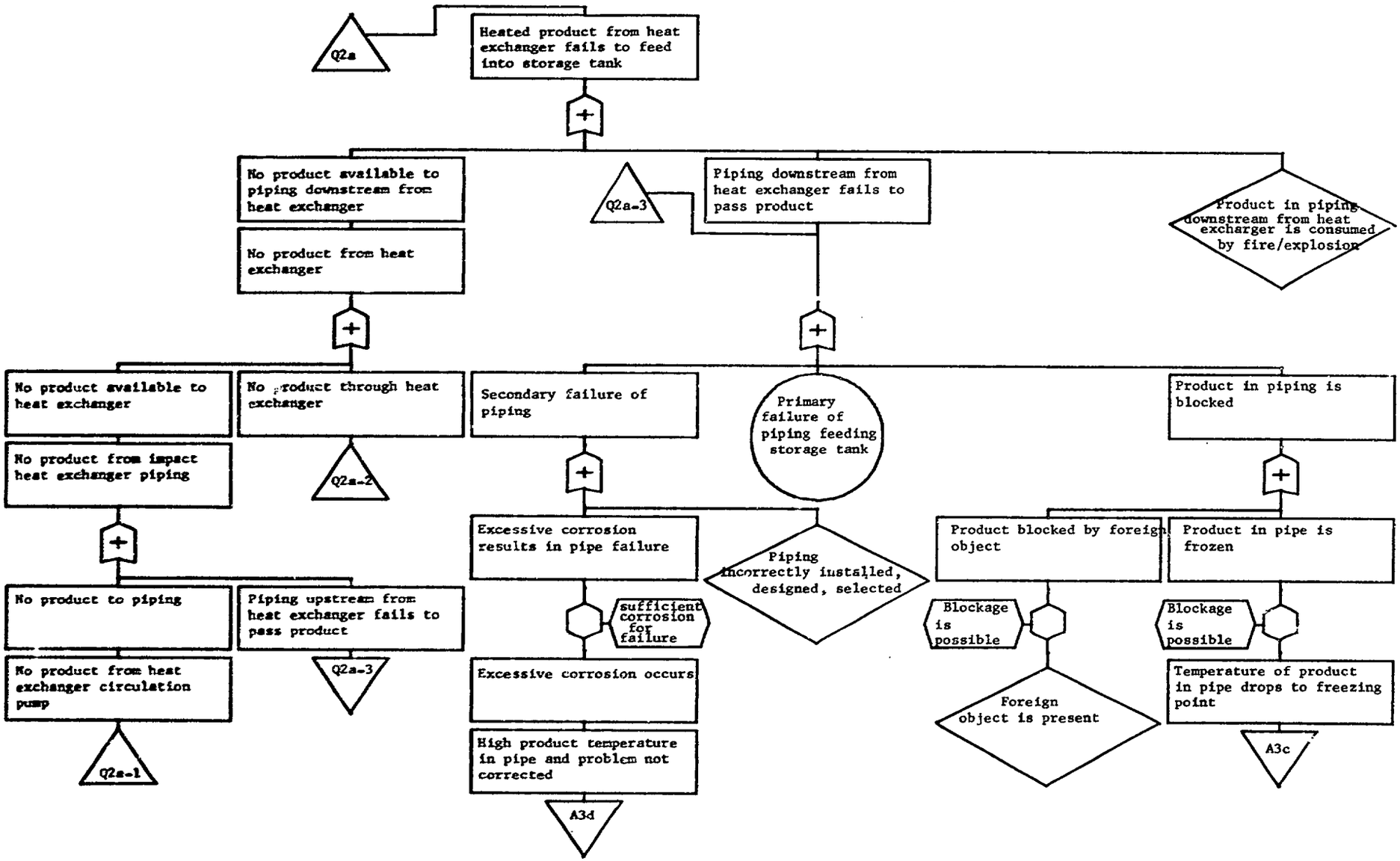

Pipeline between new pumphouse and storage tank fails to pass product
Primary failure of pipe
Secondary failure of pipe
A3-2
Product blockage in pipe
A3-1

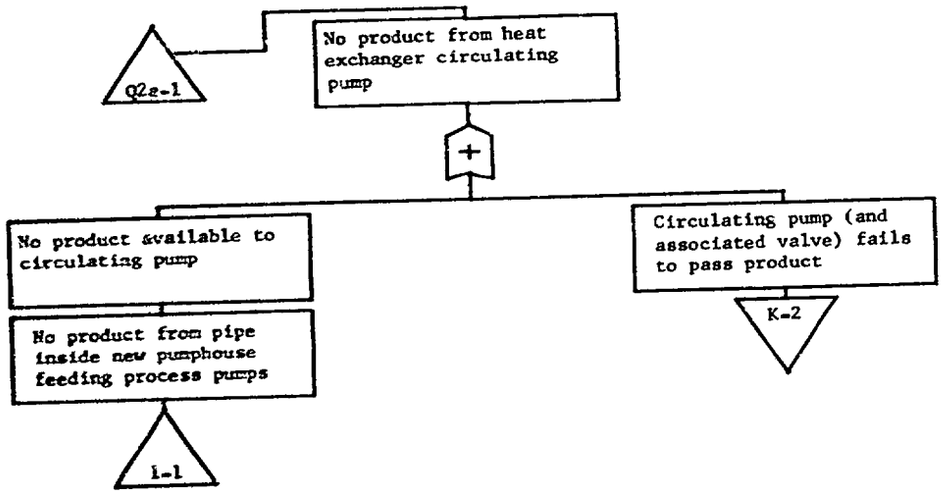

P
Product consumed by fire/ explosion in pipeline between new pumphouse and storage tank
Explosion in pipeline between new pumphouse and storage tank
Transition to explosion
Fire in pipeline between new pumphouse and storage tank
P-1
Fire in pipeline between new pumphouse and storage tank
P-1
Sufficient initiation stimulur to cause fire in pipeline
Combustible material present
Sufficient thermal stimulus to cause cookoff in pipeline
Cookoff temp. reached
High product temp. in pipeline between new pumphouse and storage tank
Excessive heating from steam tracing and problem not corrected
A3d

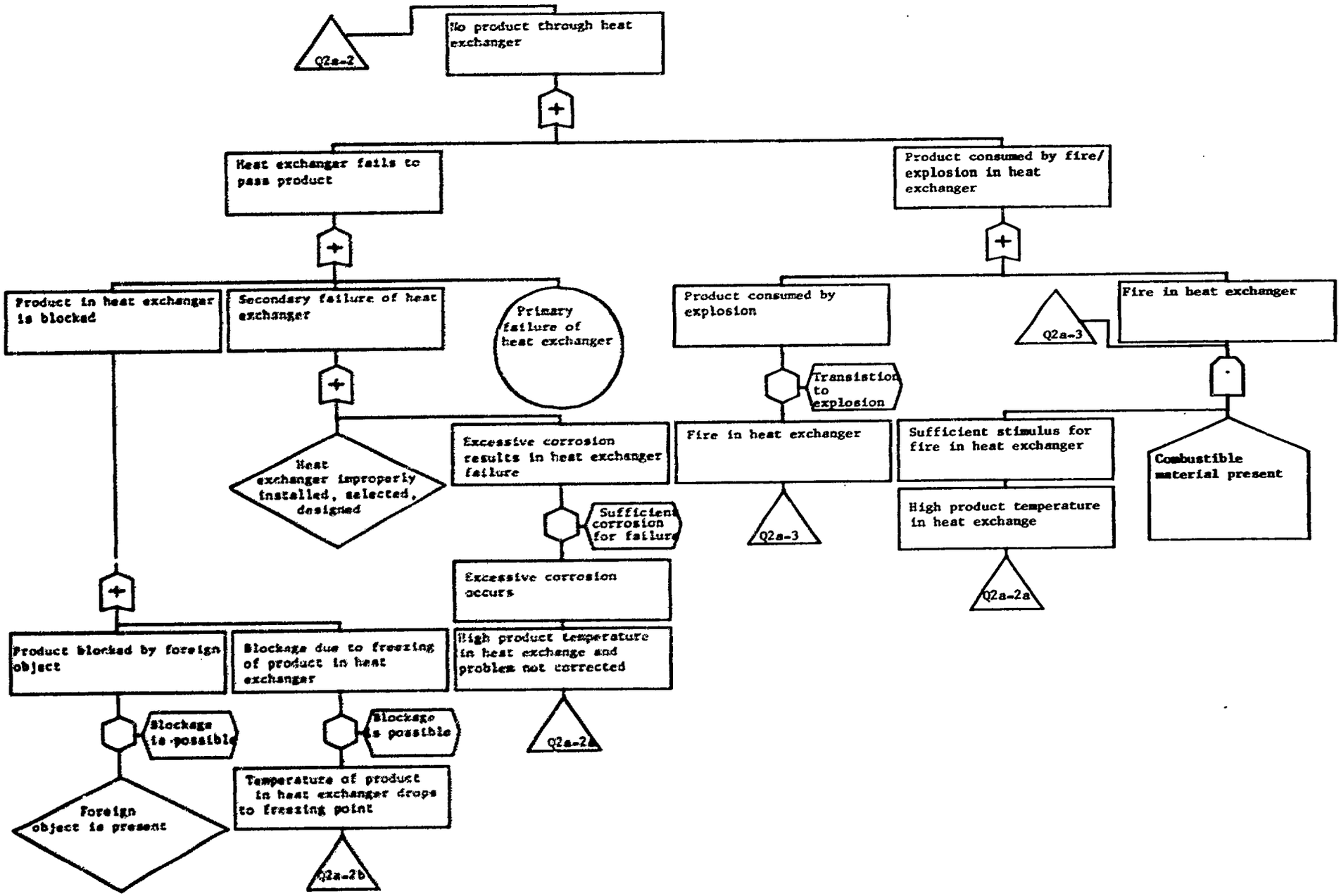

Q
New storage tank fails to pass product
Secondary failure of storage tank
Blockage of product in storage tank
Primary failure of storage tank
Product is frozen in tank
Excessive corrosion results in storage tank failure
Tank improperly designed, installed, selected, etc.
Blockage is possible
Suff. corrosion for failure
Product temperature in tank drops to freezing point before low temp. is corrected
Excessive corrosion occurs
High product temperature in storage tank
Q-4
Product temperature drops to abnormal low level in storage tank
Product temperature not corrected by bayonet heater
Insufficient heat input into storage tank
Q1
Q2
High heat impact into storage tank
Problem not corrected by operator
Operator is unaware of improper product temp. in storage tank
Abnormal amount of steam through TCV of tanks bayonet heater
Excessive heating from heat exchanger
Q 3
Q1-1
Q2b

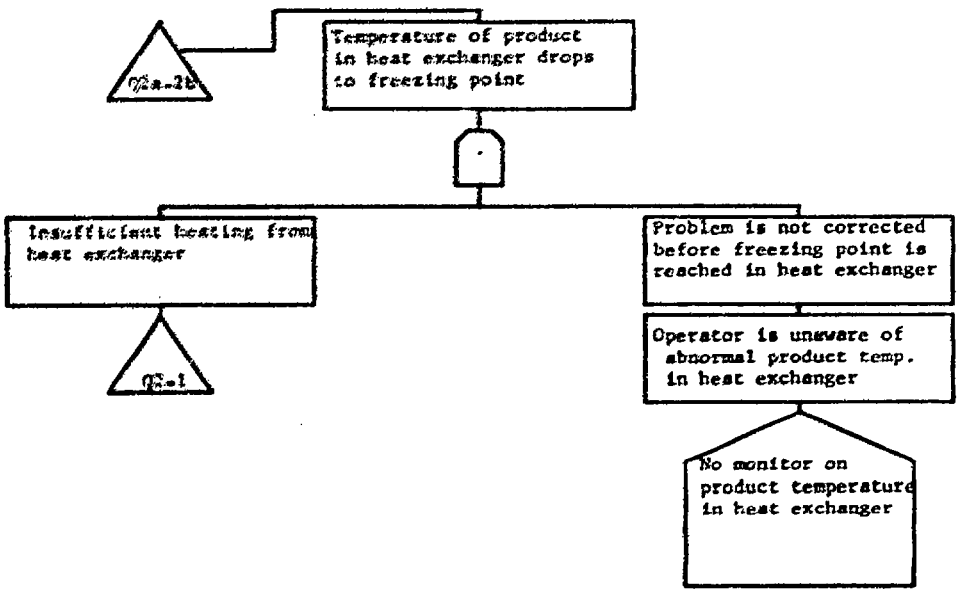

Q1
Heater is employed but product temperature is not raised
Abnormal amount of steam to bayonet heater
Secondary failure of immersion heater
Primary failure of immersion heater
Abnormal amount of steam from TCV of bayonet heater
Heater improperly designed, installed, etc.
Abnormal amount of steam to TCV
Abnormal amount of steam through TCV
Q1-1
Incorrect design, installation of steam piping
Command failure of bayonet TCV
Secondary failure of valve
Primary failure of valve
TT fails to send signal to TCV
Improper design, selection, installation of valve
Secondary failure of TT
Primary failure of TT
TT incorrectly installed, designed, selected

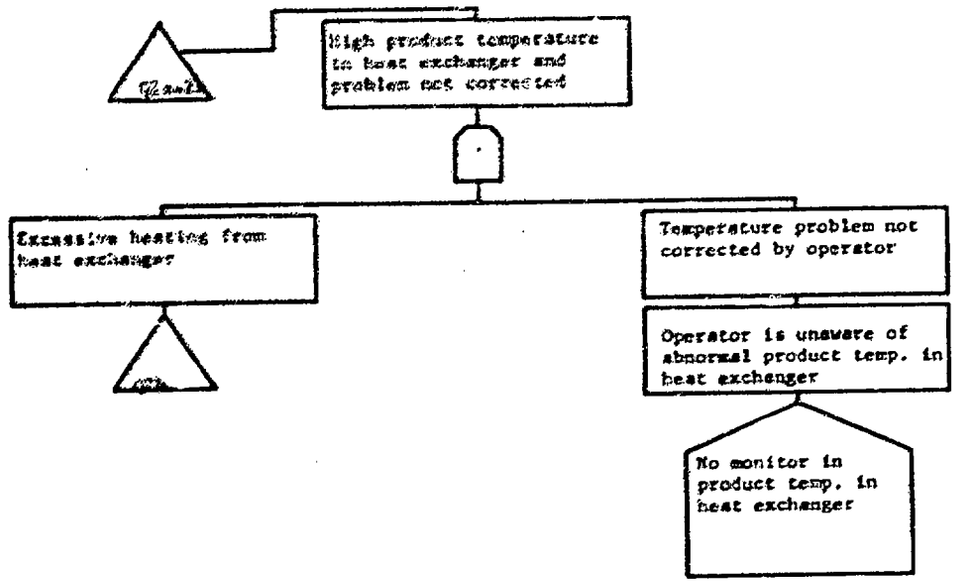

Q2
Insufficient heat input into stroage tank
An abnormally large heat requirement can not be met by the heat exchange as designed
Abnormal requirement design capability
Abnormally large amount of heat is required from heat exchange
Operator of the heat exchanger fails to meet the normal heating requirments of storege tank
Q2-1
Heated product from heat exchanger fails to feed into storage tank
Q2a
Insufficient steam to heat exchanger
Secondary failure of heat exchanger
Primary failure of heat exchanger
Heat exchanger improperly designed, installed, selected
Insufficient steam to TCV-3
Insufficient steam through TCV-3
I2-1
Abnormal steam flow through TCV-3
Q2b
Abnormally large amount of heat from heat exchange is required by piping
Excessive amount of heat is lost from storage tank
Inadequate heating from steam tracing
AC3-1
Secondary failure of pipe insulation
Primary failure of pipe insulation
Pipe insulation impingement designed, installed, etc.
Tank insulation improperly designed, installed, etc.
Primary failure of tank insulation

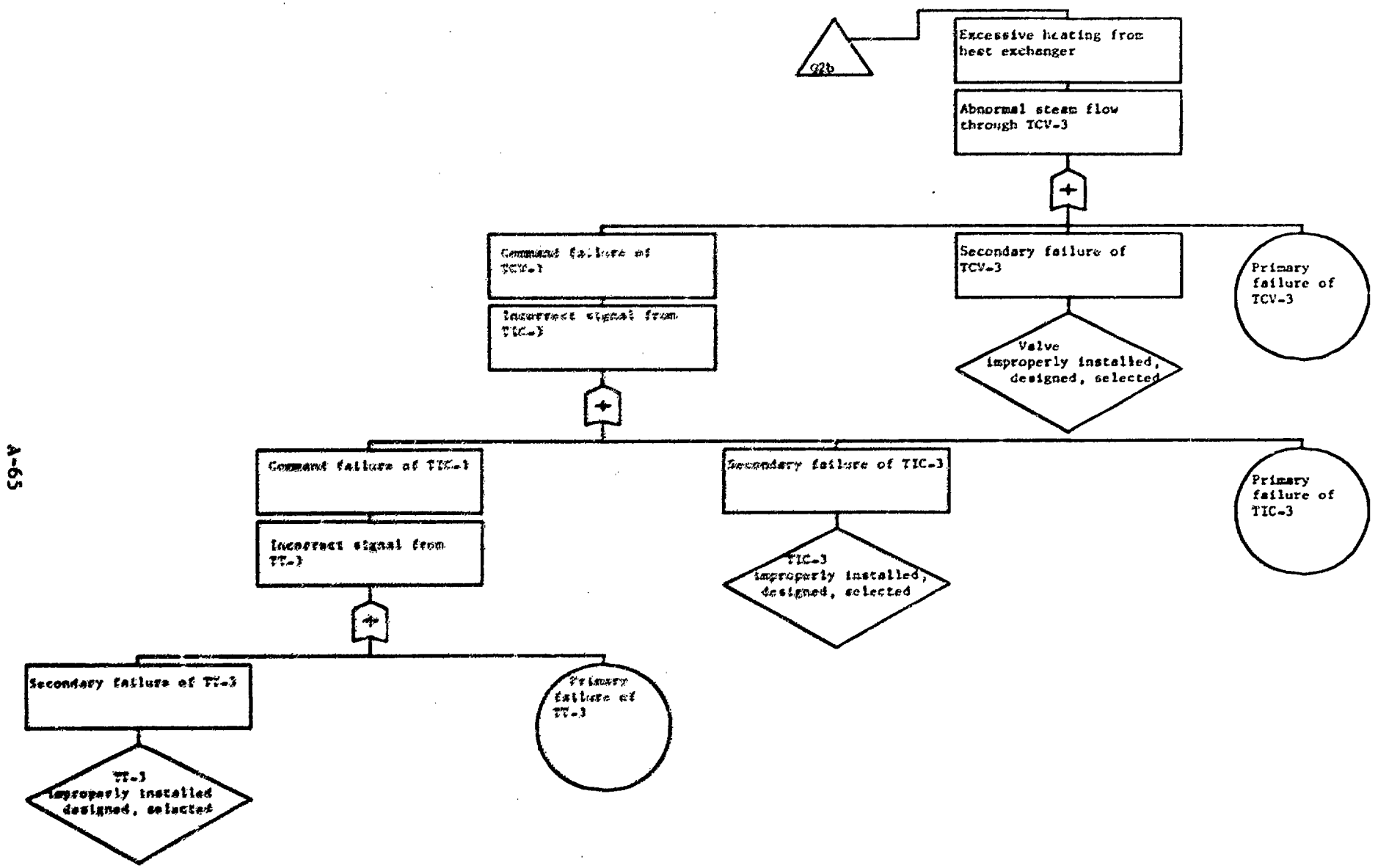

Q2a
Heated product from heat exchanger fails to feed into storage tank
No product available to piping downstream from heat exchanger
No product from heat exchanger
Q2a-3
Piping downstream from heat exchanger fails to pass product
Product in piping downstream from heat excharger is consumed by fire/explosion
No product available to heat exchanger
No product from impact heat exchanger piping
No product to piping
No product from heat exchanger circulation pump
Q2a-1
No product through heat exchanger
Q2a-2
Piping upstream from heat exchanger fails to pass product
Q2a-3
Secondary failure of piping
Excessive corrosion results in pipe failure
sufficient corrosion for failure
Excessive corrosion occurs
High product temperature in pipe and problem not corrected
A3d
Primary failure of piping feeding storage tank
Piping incorrectly installed, designed, selected
Product in piping is blocked
Product blocked by foreign object
Blockage is possible
Foreign object is present
Product in pipe is frozen
Blockage is possible
Temperature of product in pipe drops to freezing point
A3c

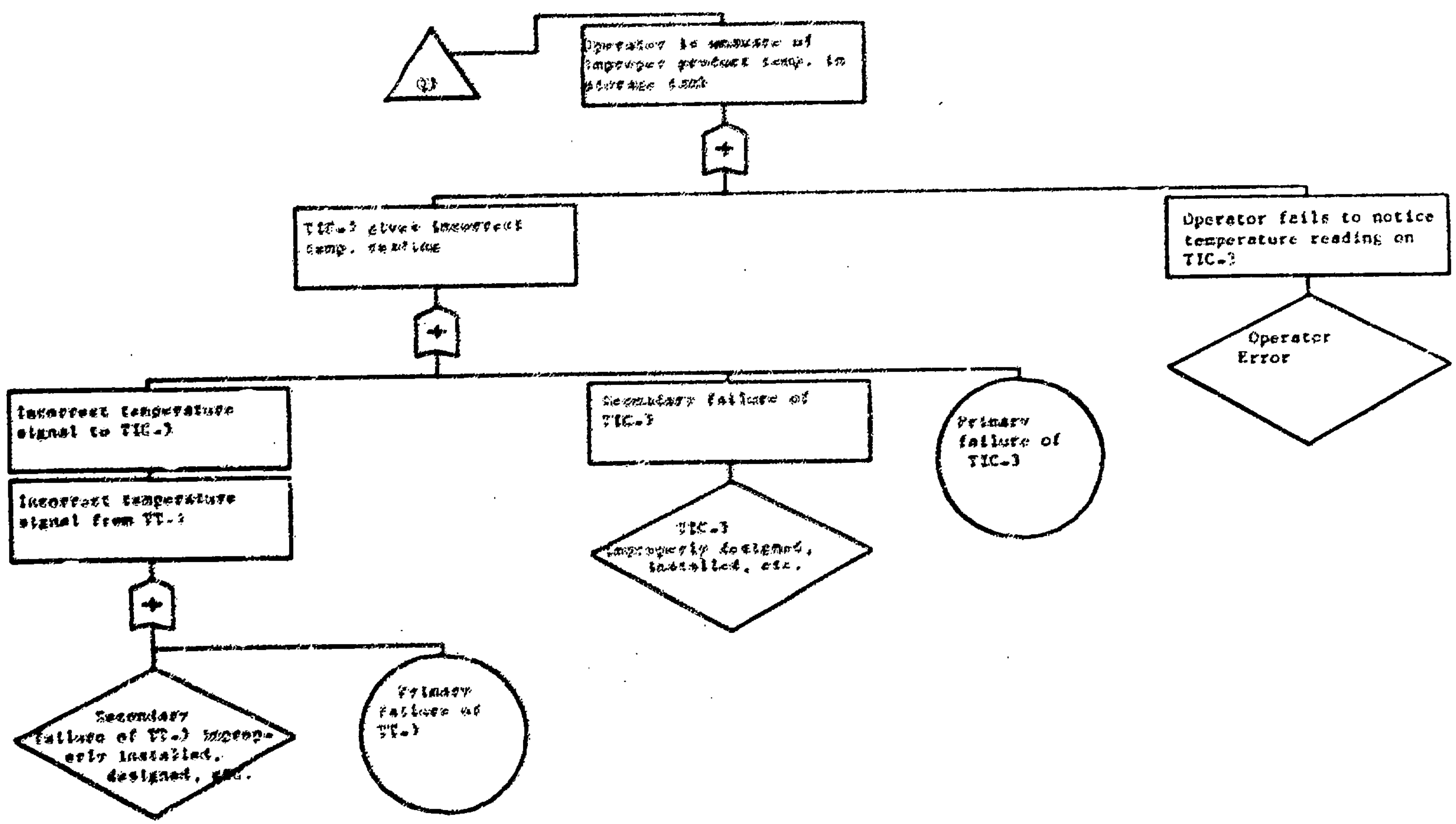

Q2e-1
No product from heat exchanger circulating pump
+
No product available to circulating pump
Circulating pump (and associated valve) fails to pass product
No product from pipe inside new pumphouse feeding process pumps
K-2
i-1

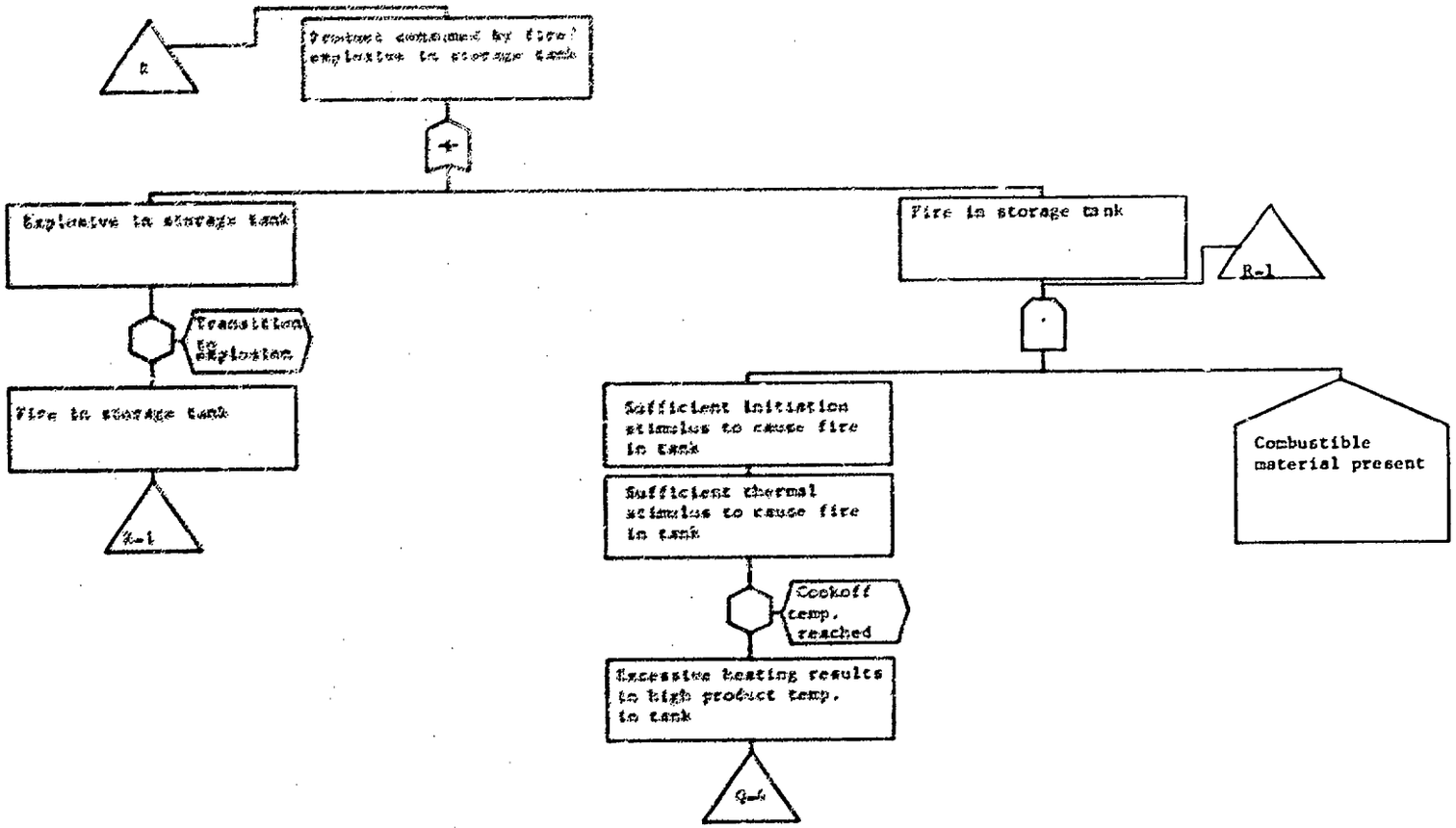

No product through heat exchanger
Q2a-2
Heat exchanger fails to pass product
Product consumed by fire/ explosion in heat exchanger
Product in heat exchanger is blocked
Secondary failure of heat exchanger
Primary failure of heat exchanger
Product consumed by explosion
Q2a-3
Fire in heat exchanger
Transistion to explosion
Heat exchanger improperly installed, selected, designed
Excessive corrosion results in heat exchanger failure
Fire in heat exchanger
Sufficient stimulus for fire in heat exchanger
Combustible material present
Sufficient corrosion for failure
Q2a-3
High product temperature in heat exchange
Q2a-2a
Excessive corrosion occurs
Product blocked by foreign object
Blockage due to freezing of product in heat exchanger
High product temperature in heat exchange and problem not corrected
Blockage is possible
Blockage is possible
Q2a-2
Temperature of product in heat exchanger drops to freezing point
Foreign object is present
Q2a-2b

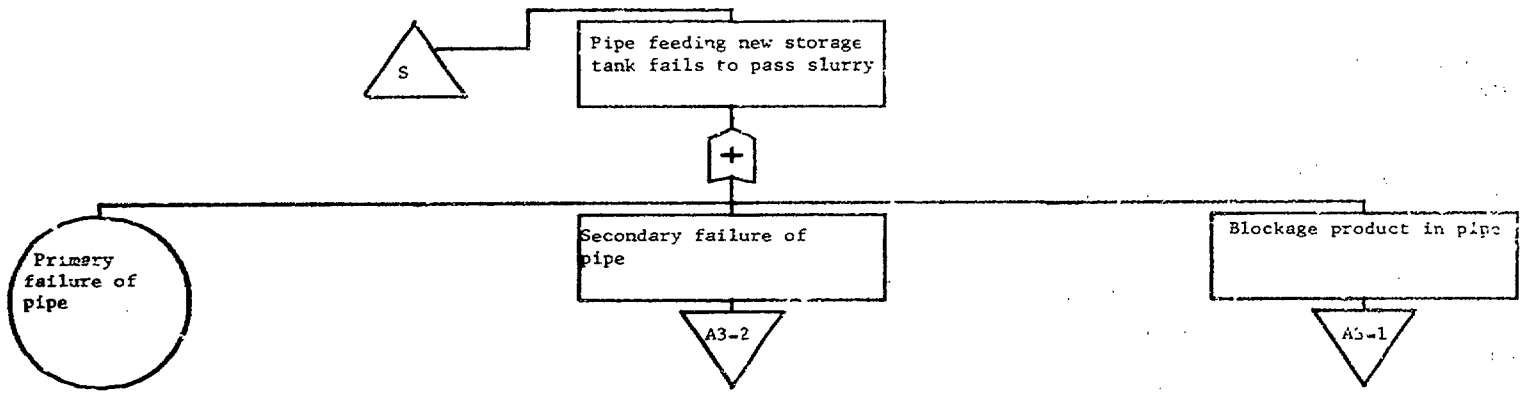

Temperature of product in heat exchanger drops to freezing point
Insufficient heating from heat exchanger
Problem is not corrected before freezing point is reached in heat exchanger
Operator is unaware of abnormal product temp. in heat exchanger
No monitor on product temperature in heat exchanger

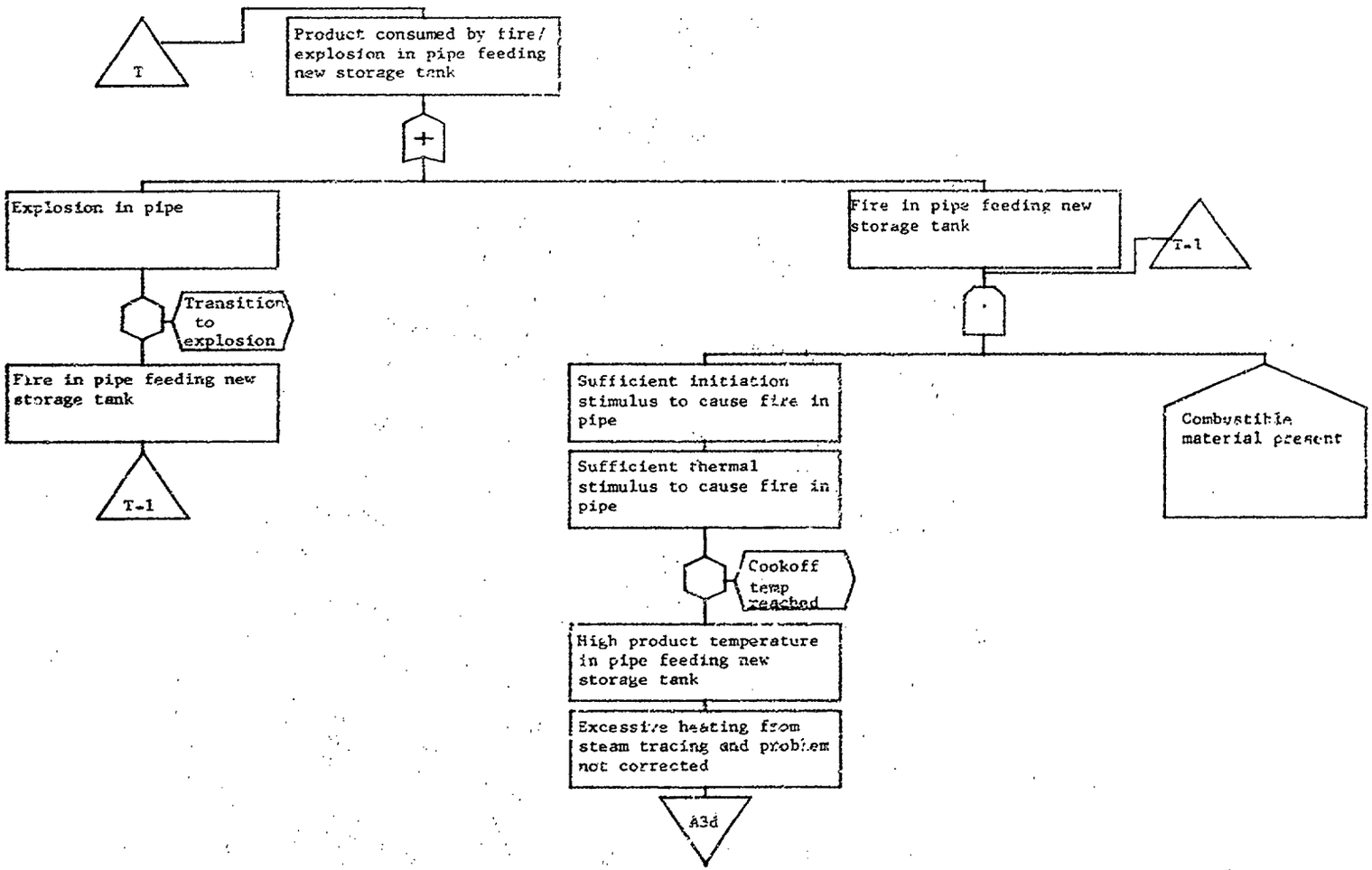

High product temperature in heat exchanger and problem not corrected
Excessive heating from heat exchanger
Temperature problem not corrected by operator
Operator is unaware of abnormal product temp. in heat exchanger
No monitor in product temp. in heat exchanger

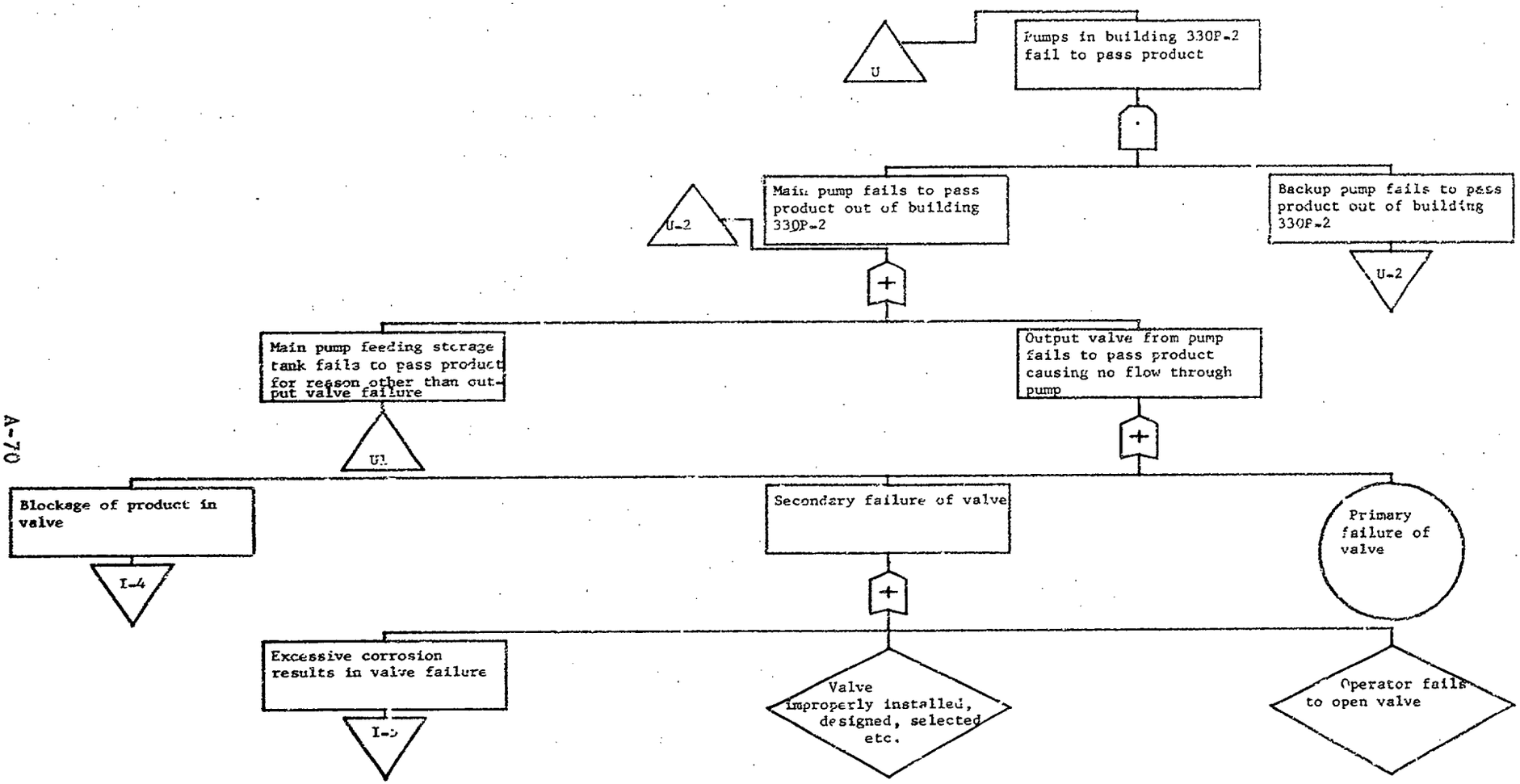

92b
Excessive heating from heat exchanger
Abnormal steam flow through TCV-3
Command failure of TCV-3
Incorrect signal from TIC-3
Secondary failure of TCV-3
Primary failure of TCV-3
Valve improperly installed, designed, selected
Command failure of TIC-3
Incorrect signal from TT-3
Secondary failure of TIC-3
Primary failure of TIC-3
TIC-3 improperly installed, designed, selected
Secondary failure of TT-3
Primary failure of TT-3
TT-3 improperly installed designed, selected

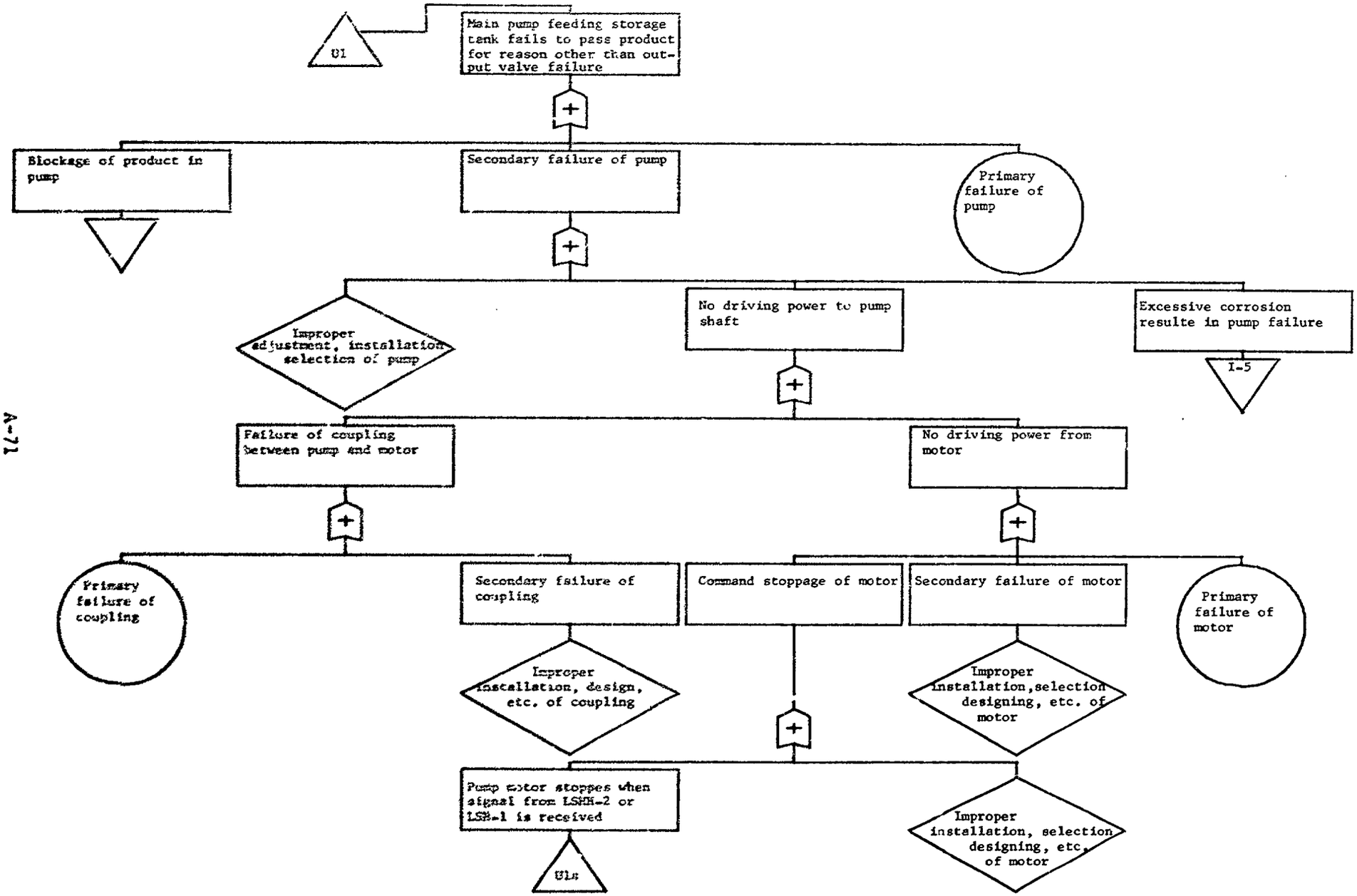

Operator is unaware of improper product temp. in storage tank
TIC-3 gives incorrect temp. reading
Operator fails to notice temperature reading on TIC-3
Operator Error
Incorrect temperature signal to TIC-3
Incorrect temperature signal from TT-3
Secondary failure of TIC-3
Primary failure of TIC-3
TIC-3 improperly designed, installed, etc.
Secondary failure of TT-3 improperly installed, designed, etc.
Primary failure of TT-3

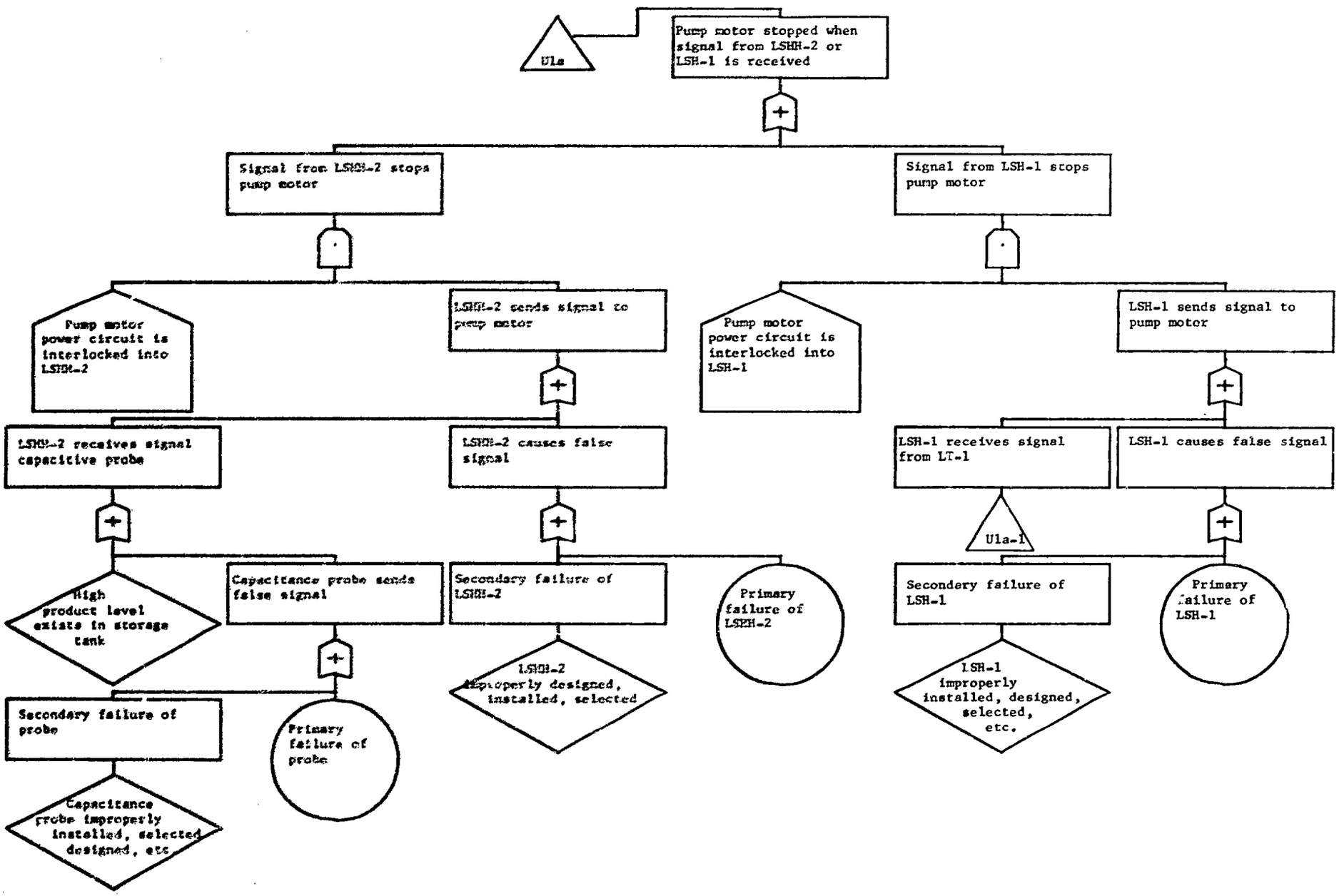

Explosive in storage tank
Transition to explosion
Fire in storage tank
Fire in storage tank
R=1
Sufficient initiation stimulus to cause fire in tank
Sufficient thermal stimulus to cause fire in tank
Cookoff temp. reached
Excessive heating results in high product temp. in tank
Combustible material present

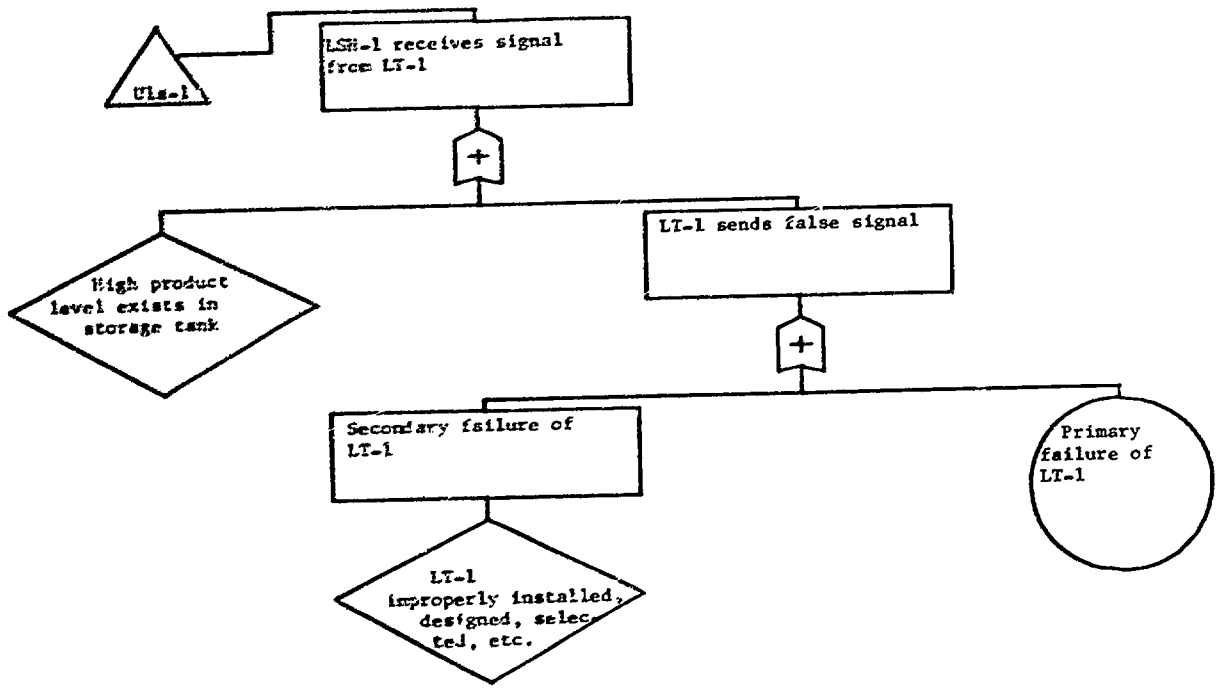

S
Pipe feeding new storage tank fails to pass slurry
Primary failure of pipe
Secondary failure of pipe
Blockage product in pipe
A3-2
A3-1

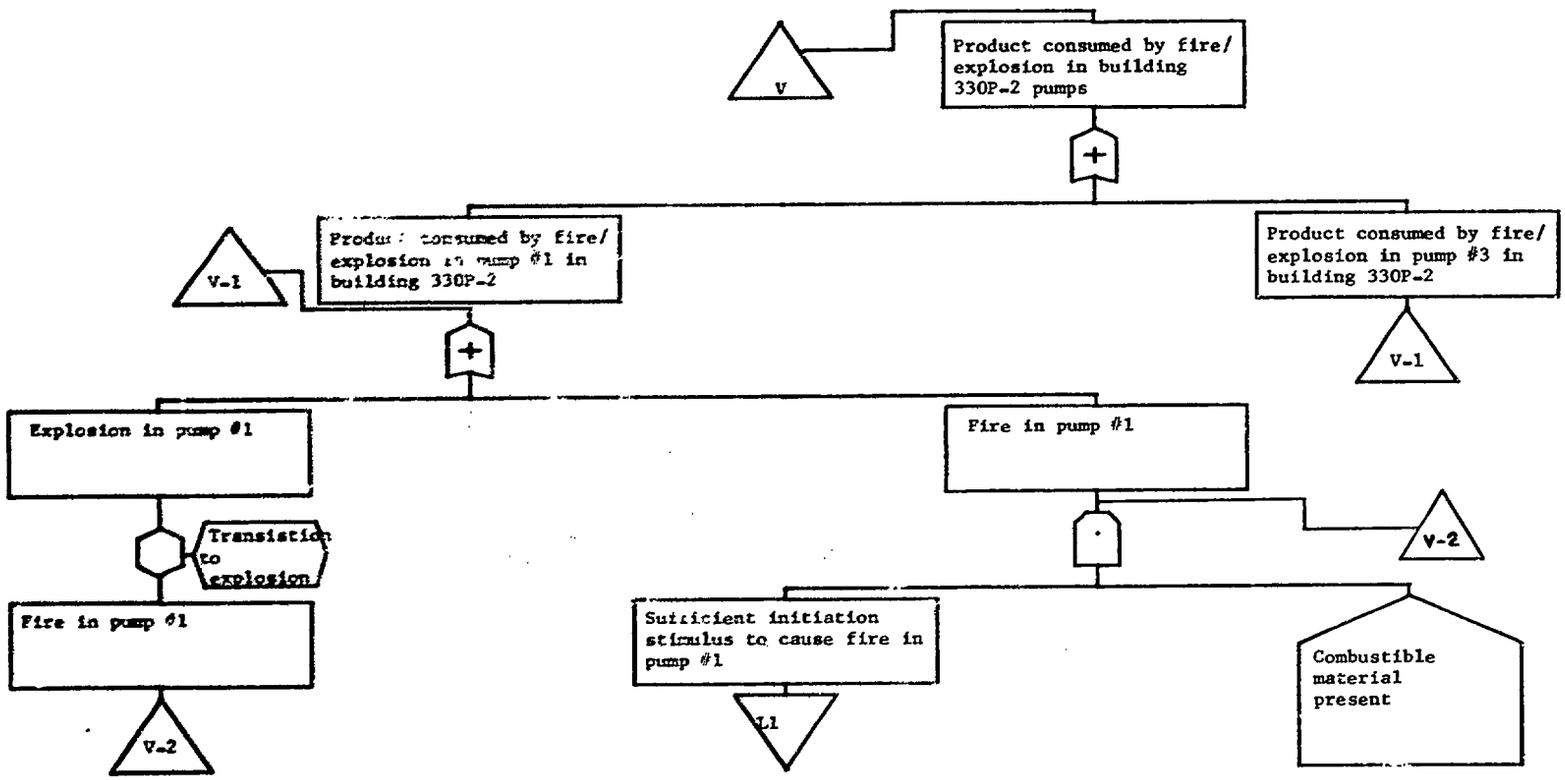

T
Product consumed by fire/ explosion in pipe feeding new storage tank
Explosion in pipe
Transition to explosion
Fire in pipe feeding new storage tank
T-1
Fire in pipe feeding new storage tank
T-1
Sufficient initiation stimulus to cause fire in pipe
Sufficient thermal stimulus to cause fire in pipe
Cookoff temp reached
High product temperature in pipe feeding new storage tank
Excessive heating from steam tracing and problem not corrected
A3d
Combustible material present


U
Pumps in building 330P-2 fail to pass product
U-2
Main pump fails to pass product out of building 330P-2
Backup pump fails to pass product out of building 330P-2
U-2
Main pump feeding storage tank fails to pass product for reason other than output valve failure
Output valve from pump fails to pass product causing no flow through pump
U1
Blockage of product in valve
I-4
Secondary failure of valve
Primary failure of valve
Excessive corrosion results in valve failure
I-5
Valve improperly installed, designed, selected etc.
Operator fails to open valve


U1
Main pump feeding storage tank fails to pass product for reason other than output valve failure
Blockage of product in pump
Secondary failure of pump
Primary failure of pump
Improper adjustment, installation selection of pump
No driving power to pump shaft
Excessive corrosion resulte in pump failure
I-5
Failure of coupling between pump and motor
No driving power from motor
Primary failure of coupling
Secondary failure of coupling
Command stoppage of motor
Secondary failure of motor
Primary failure of motor
Improper installation, design, etc. of coupling
Improper installation,selection designing, etc. of motor
Pump motor stoppes when signal from LSHH-2 or LSH-1 is received
Improper installation, selection designing, etc. of motor
U1a


U1a
Pump motor stopped when signal from LSHH-2 or LSH-1 is received
Signal from LSHH-2 stops pump motor
Signal from LSH-1 stops pump motor
Pump motor power circuit is interlocked into LSHH-2
LSHH-2 sends signal to pump motor
Pump motor power circuit is interlocked into LSH-1
LSH-1 sends signal to pump motor
LSHH-2 receives signal capacitive probe
LSHH-2 causes false signal
LSH-1 receives signal from LT-1
LSH-1 causes false signal
U1a-1
High product level exists in storage tank
Capacitance probe sends false signal
Secondary failure of LSHH-2
Primary failure of LSHH-2
Secondery failure of LSH-1
Primary failure of LSH-1
LSHH-2 improperly designed, installed, selected
LSH-1 improperly installed, designed, selected, etc.
Secondary failure of probe
Primary failure of probe
Capacitance probe improperly installed, selected designed, etc.


Uls-1
LSH-1 receives signal from LT-1
+
High product level exists in storage tank
LT-1 sends false signal
+
Secondary failure of LT-1
Primary failure of LT-1
LT-1 improperly installed, designed, selected, etc.


V
Product consumed by fire/ explosion in building 330P-2 pumps
V-1
Product consumed by fire/ explosion in pump #1 in building 330P-2
Product consumed by fire/ explosion in pump #3 in building 330P-2
V-1
Explosion in pump #1
Fire in pump #1
Transistion to explosion
V-2
Fire in pump #1
Sufficient initiation stimulus to cause fire in pump #1
Combustible material present
V-2
L1

APPENDIX B

EXPERIMENTAL DISCUSSION

Material response testing for this program was conducted in accordance with Hercules procedures. The specific details of each test procedure have not been included in this report since most of the tests are fully described in the literature.[15] Any specific questions concerning any of the tests or experimental results discussed previously in this report should be directed to ABL.

The following is a brief description of each of the tests used to obtain the material response data for this program:

1. Impact

Impact testing of process materials was conducted on the ABL impact machine. The ABL impact machine is designed to deliver controlled energy from a falling weight retained in guide bars, through an intermediate hammer, to the test material resting on an anvil. The machine provides a valid means of obtaining initiation data by impacting a small sample. The data obtained reflect the effects of velocity, hammer area, particle size, sample thickness, materials of construction, sample temperature and sample confinement.

Initiation is detected by observing odor, stain, smoke, sample scattering, noise, etc. When any doubt exists concerning initiation detection, the

limits of the operator's judgment are extended through the use of an infrared analyzer. This device is capable of detecting decomposition products, including such gases as CO, CO_2, NO_2 and N_2O, between 4-5 microns in the spectra wavelength with a sensitivity limit of about 40 parts/million.

2. Friction

Friction testing was conducted on the ABL Model I Sliding Friction machine, a pendulum-driven device. This machine is a versatile device which is capable of determining the initiation response of explosive materials to friction over a wide range of conditions. The machine can duplicate almost any frictional situation with respect to frictional force, velocity, sliding distance, materials of construction involved, and environment.

3. Electrostatic Discharge

The electrostatic discharge test is designed to determine the response of sensitive materials to various electrostatic discharge energy levels. The material to be tested is placed within a grounded sample container, and electrostatic energies of various known magnitudes are passed from a point source through the sample until a maximum energy which will not result in initiation in 20 successive trials is established. Energy sources consist of charged capacitors as well as the energy delivered by a human spark.

4. Particle Impingement

This test is designed to simulate pumping of explosive liquids by impinging various sized samples up to velocities of ~ 40,000 fpm onto a target. Initiation is detected by either a Polaroid camera to record initiation flashes or a force gage.

5. Transition

The transition test consists of subjecting explosive materials to bottom flame initiation from a 12 gram (6 gram FFFG and 6 gram 2056 casting powder) bag igniter. The explosive is placed in schedule 40 pipe, and pipe diameter and length are varied to obtain a relationship between confinement diameter and critical height to explosio The critical height is that level above which explosions will occur as a result of 3 failures at that level. Standard container diameters are 1, 2 and 4 inch pipe.

6. Explosive Propagation

This test is designed to determine the minimum diameter above which process materials will propagate a high order reaction when confined in a 24" long steel pipe. The booster material employed as the detonation source is Comp. C-4. Detection method consists of a lead plate with Primacord, in addition to visible inspection.

7. Sustained Reaction (Fire)

This test consists of exposing a 1/2 inch thick layer of material to an energetic ignition source (thermite igniter or Atlas match) to determine if a sustained burning results. The material is held in an 8" long aluminum tray and the igniter is placed inside the tray, at the bottom of the test material. Visual observation of the material after ignition determines the extent of the burning reaction.

APPENDIX C

RELIABILITY CALCULATIONS

The probability of a component failing after a given time interval in hours is calculated as follows:

$$\text{Probability of Failure} = 1 - e^{-(\text{Failure Rate}) \times (\text{Hours})}$$

$$= (\text{Failure Rate}) \times (\text{Hours})$$

For example, if failure rate is 5×10^{-6} and the time interval is 2160 hours, the probability of failure is:

$$\text{Probability of Failure} = (1 - e)^{-(5 \times 10^{-6}) \times (2160)}$$

$$= (5 \times 10^{-6}) \times (2160)$$

$$= 0.0108$$

For two components to fail simultaneously:

$$\text{Probability of failure} = (1-e^{-\lambda_1 t_1})\ (1-e^{-\lambda_2 t_2})$$

$$= (\lambda_1 t_1)\ (\lambda_2 t_2)$$

$$= \lambda_1\ \lambda_2\ (\text{time})^2$$

For example, if $\lambda_1 = (3.01 \times 10^{-6}) \lambda_2 = 2 \times 10^{-6}$, $t = 2160$ hours

then, $\lambda_1 t = (3.0 \times 10^{-6})\ (2160) = 6.48 \times 10^{-3}$

$\lambda_2 t = (2.0 \times 10^{-6})(2160) = 4.32 \times 10^{-3}$

$\lambda_{1t}\ \lambda_{2t} = (3.0 \times 10^{-6})\ (2 \times 10^{-6})\ (2160)^2$

$= (6 \times 10^{-12})\ (4.7656 \times 10^{6})$

$= 2.8 \times 10^{-5}$

This example indicates that the single factor failure mode gives probabilities, of failure of 6.5×10^{-3} and 4.3×10^{-3}, while the probability that they will fail simultaneously is 2.8×10^{-5}. Thus, a single factor failure mode is approximately 100 times, more severe($= 10^{-3}$ vs $= 10^{-5}$ probability) than two factor failure modes, or it requires approximately 100 two factor failure modes to be equivalent to one single factor failure mode. (For a further discussion of mathematical treatment of this subject, see reference 18.)

This low contribution of two factor failure modes was also the justification for merely adding the probabilities of failure. That is, conventional probability theory for adding of probabilities is as follows:

$$P(\epsilon_1 + \epsilon_2 + \epsilon_3 + \cdots + \epsilon_r) = \sum_{i=1}^{r} P(\epsilon_i) = \sum_{i=1}^{r} \sum_{\substack{j=1 \\ (i \neq j)}}^{r} P(\epsilon_i)\, P(\epsilon_j) \pm \text{higher order terms}$$

However, as was numerically illustrated, the contribution of the two factor failure modes may be neglected since they are very small in relation to the single factors. Thus,

$$\sum_{i=j}^{r} \sum_{j=i}^{r} P(\epsilon_i)\, P(\epsilon_j) = 0 \text{ (all other higher order terms are zero also).}$$

$$\text{or } P(\epsilon_1 + \epsilon_2 + \epsilon_3 + \cdots + \epsilon_r) = P(\epsilon_1) + P(\epsilon_2) + P(\epsilon_r) + \cdots + P(\epsilon_r)$$

$$= \sum_{i=i}^{r} P(\epsilon_i)$$

APPENDIX D

CALCULATION OF ADIABATIC FLAME TEMPERATURE FOR AN

The most favorable decomposition reaction path for AN from a free energy standpoint is:

$$NH_4NO_3 \longrightarrow 2H_2O + N_2 + 1/2\ O_2 \quad (9,16)$$

which liberates 28,470 calories/g-mole AN[10], with all products in the gaseous state at 25°C.

$$q = (1 \text{ lb-mole } NH_4NO_3)\ (28{,}470 \text{ cal/g-mole})\ \left(\frac{454 \text{ g-mole}}{\text{lb-mole}}\right)\ \left(\frac{1 \text{ Btu}}{252 \text{ cal}}\right)$$

$$= 5.14 \times 10^4 \text{ Btu}$$

The heat balance is:

$$q = n_{N_2} Cp_{N_2} (T - 77°F) + n_{O_2} Cp_{O_2} (T - 77) + n_{H_2O} Cp_{H_2O(g)} (T - 77)$$

where

n_{N_2} = 1.0 lb-mole

n_{O_2} = 0.5

n_{H_2O} = 2.0

Cp_{N_2} = 7.2 Btu/lb-mole °F (Heat capacity at a temperature of 1000°F for all gases)

Cp_{O_2} = 7.6

$Cp_{H_2O(g)}$ = 8.7 Btu/lb-mole °F

$$5.14 \times 10^4 = 1.0(7.2)(T - 77) + 0.5(7.6)(T - 77) + 2.0(8.7)\ (T - 77)$$

$$T = 1890°F$$

Since the minimum temperature for a flame is 1500°K[17] or 2241°F, there is no possibility of a flame occurring with pure AN.

The particular decomposition reactio path employed in this analysis is, from a free energy standpoint, the most favorable. It is possible, indeed likely, that additional decomposition reactions may also occur. One alternative reaction suggested by Holston involves the formation of nitrous oxide, dinitrogen tetroxide, and water as decomposition products:

$$NH_4NO_3 \longrightarrow 1/3\ N_2O + 1/6\ N_2O_4 + 2\ H_2O + 1/2\ N_2$$

The heat of reaction of this equation is calculated (via heat of formation considerations) to be about 20,634 cal/g-mole. Using a similar "heat balance" approach employed above, an adiabatic flame temperature of 835°F is calculated. This value is again well below the 2241°F minimum temperature level required for a flame to occur.